

ATS8600
User Guide
Version ATS8600 2014 SP1

Table of Contents

1 Introduction	7
1.1 ATS8600 Integrated Security Management System characteristics	7
1.2 Technical specifications	9
1.3 Security of Integrated Security Management System.....	10
2 Operating procedures	11
2.1 Integrated Security Management System start-up	11
2.2 Structure of the Professional panel.....	11
2.2.1 Main menu	12
2.2.1.1 System restart.....	13
2.2.2 Tree	13
2.2.2.1 The tree tab	13
2.2.3 Toolbar	13
2.2.4 Infotypes Panel and its tabs	14
2.2.5 Navigation Panel and its tabs	14
2.2.6 System information	15
2.2.7 RT status (Real-Time system heartbeat)	15
2.3 Working in the Professional view.....	15
2.3.1 Working with the tree	15
2.3.2 Confirming and saving changes	17
2.3.3 Function selection in the tree	17
2.3.4 Search	18
3 User management	20
3.1 Entering start date and end date of access.....	20
3.2 Creating the organizational structure	21
3.2.1 Adding the company to the OS	21
3.2.2 Adding a department to the OS	22
3.2.3 Adding other types of record to the OS	22
3.2.4 Changing an OS record	23
3.2.5 Importing the Image to the Person's Record	23
3.2.6 Deleting the Record	23
3.2.7 Group management in the OS	26
3.2.7.1 Creating the group	26
3.2.7.2 Adding an Object into a Group.....	26

3.2.7.3	Removing an Object from a Group.....	28
3.3	Credentials Management in OS Environment.....	28
3.3.1	Types of credentials	29
3.3.2	Card Management	30
3.3.3	Assign to administration	32
3.3.4	Creating a card	34
3.3.5	Assigning a Card to its Owner	34
3.3.6	Learning new cards directly from a device	35
3.3.7	Creating a non-transferrable credential	37
3.3.8	Merging credentials	37
3.3.9	Credential Status	39
3.3.10	Credential activation	39
3.3.11	Credential removal	40
3.3.12	Deleting a card	40
3.4	Role assignment	41
3.4.1	Descriptions of Roles	41
3.5	Personal Settings	48
3.5.1	Setting access to the Application	48
3.5.2	Administration of personal settings	50
3.6	Permissions management	51
3.6.1	Permissions group settings	52
3.6.2	Types of permission	53
3.6.3	Permission state	59
3.6.4	Principle of inheriting	60
3.6.5	Permission setting	61
3.6.6	Example of configuring permissions	62
3.7	Access	72
3.7.1	Allowing access to devices	73
3.7.2	Allowing access to regions	73
3.7.3	Time Restrictions	74
3.7.4	Holidays	77
3.7.4.1	Import of Holiday Definition from a File.....	78
3.7.4.2	Entering Holidays Manually.....	80
3.7.5	Access report	81
4	Extended properties	83
5	ATS8600 Device Manager	84
6	Device Management	85
6.1	Adding a device	85

6.2	Running a device	86
6.3	Changing the device type.....	87
6.4	Device statuses	88
6.4.1	Device statuses filter	89
7	Regions	93
7.1	Create regions	93
7.2	Device structure in a region.....	94
7.2.1	Allowing access in the Regions tree	97
7.2.2	Number of persons in the region	97
8	Assets	100
8.1	Automatic reports print set-up.....	103
9	Replications	104
9.1	Connector to external IS.....	104
9.2	Replication settings.....	106
9.2.1	Confirming the replication	107
9.2.2	Event monitoring	109
10	Visualization	111
10.1	Example of visualisation	113
10.2	Auxiliary windows description.....	120
10.2.1	Regions	121
10.2.2	Objects window	121
10.2.3	Devices window	121
10.2.4	Properties window	121
10.2.5	Patrols window	121
10.3	Properties of visualisation elements.....	122
10.4	Alarm propagation.....	124
10.5	Adding a Button in visualization	124
10.6	Mask editor	126
10.7	PTZ module	129
10.7.1	Creating a link between the mask and the device	129
11	Monitor	132
11.1	Monitor panel windows	135
11.1.1	Events window	135
11.1.2	Event history window	136
11.1.3	Alarm management window	137
11.1.4	Persons present window	140

11.1.5 Status Filter window	140
11.1.6 Video storyboard window	140
11.2 Alarm sounds	141
11.3 Device Remote Control.....	142
11.4 Connecting a camera to a device.....	142
11.5 Automatic Camera Live Screen View in the Monitor Panel.....	144
11.6 Controlling PTZ Cameras.....	146
11.7 Overall enabling or disabling of Alarm management.....	147
12 Image Monitor	148
13 Patrol tours	153
13.1 Creating and modifying a patrol.....	153
13.2 Starting and monitoring a patrol tour.....	154
14 Cash Desk Monitor	158
15 Events	160
15.1 Person related events.....	160
15.2 Device related events	162
15.3 Viewing events using regions.....	163
15.3.1 Searching for video records with events	164
15.4 Printing reports	164
15.5 Event monitoring.....	165
15.5.1 Access for authorised persons	165
15.5.2 Access denied	166
15.5.3 Using Request To Exit button	166
15.5.4 Eliminated Door	166
15.5.5 Door open too long	166
15.5.6 Remote opening of a Door	166
15.5.7 User activities	166
15.6 Event filtering	167
15.6.1 How to Create an Event Filter	168
15.6.2 Example of creating a new event filter	168
16 Automatic actions	172
16.1 Procedure for setting automatic actions.....	173
16.1.1 Automatic action owner	181
16.1.2 Test an automatic action	181
16.1.3 Automatic action script	182
16.1.4 View on the object automatic action	183

16.1.5 Running Powershell Script	184
16.2 Setting parameters	185
16.2.1 Email server	185
16.2.2 SMS gateway	186
16.2.2.1 Changing the SMS gateway Settings.....	187
17 Visits	189
17.1 Visitors management.....	189
17.1.1 Create a reception	189
17.1.2 Define accesses for reception's visitor cards	190
17.1.3 Assign visitor cards to a reception	190
17.1.4 Issuing a command for card loading	191
17.1.5 Importing visitor cards	191
17.1.6 Reception settings	191
17.1.7 Defining various access rights within one reception	192
17.2 Visitors evidence.....	194
17.2.1 Quick adding a new visit	194
17.2.2 New visitor record	195
17.2.3 Finishing the visit	197
17.2.4 Modifying visitor's data	198
18 Data import and export	200
18.1 Data export	200
18.2 Importing Data from a File.....	204
18.2.1 Person import from Microsoft Excel	206
18.2.1.1 Credentials import.....	209
19 Licensing	211
19.1 License activation.....	212
20 Diagnostics view	215
20.1 System components overview.....	215
20.2 Log management.....	215
21 Data Backup in ATS8600	217

1 Introduction

1.1 ATS8600 Integrated Security Management System characteristics

The ATS8600 Integrated Security Management System provides centralised control of security elements in companies and administrative buildings.

The ATS8600 Information System enables:

- Comprehensive management of a centrally controlled, automated building security system
- Electronic operation of connected technologies and support for security, access, camera and other systems implemented in the building
- Frequent monitoring of users' permission status, operating conditions of devices and the level of utilisation. Evaluation of monitored information.

The ATS8600 Integrated Security Management System is a tool intended for personnel management and entry control through record-keeping of Persons and their identifiers to Access rights devices.

User management - ensures the complex management of a company's hierarchical organizational structure.

Device Management - handles the registration and management of monitored add-in security devices of the system.

Region Management - enables design of logical arrangement of regions and sub-regions of ATS8600 installation with a logical device arrangement on premises. Using this arrangement it is possible to graphically represent the device arrangement in the region in the system visualization tool.

In addition, the ATS8600 personnel management and access control management provides for:

- Event management - doors status, door events, tourniquets, gates and other systems
- Definition of access rights for individuals, groups or for all users
- The possibility to restrict access rights based on time and date (including regional time zones)
- Complex history archiving of events for event evaluation purposes
- Monitoring of data related to authorized or unauthorized access attempts
- Visitor registration and permission for visitors to access the relevant region
- Online monitoring of persons in a particular time and region zones.

Through access rights managements, the ATS8600 system makes it possible to set individual or group access permissions effectively. Inherited permissions technology makes it possible to set access rights by a simple assignment of the person to the correct department or division of the company. Another advantage is the capability to perform control from one central location.

All active elements of the system are shown clearly and *hierarchically* in the device list. This list is presented in a tree and makes it possible to advise, in real time, the assigned operators of the company and security guards on duty about the status and *functionality of all operational elements* and other devices of the complete security system in the building (or buildings). Therefore, faults or violations are immediately and clearly visible in the tree, as well as on the maps of the building or sections of the building.

Deployment of ATS8600 according to the necessary guidelines, it makes it possible to manage and control everything from one location, activate or de-activate devices and to identify any violation in detail to the level of a particular room.

The interconnection of security elements with the *camera system* makes it possible to work with the camera system in real time, and to receive insight into the rooms and departments based on the connection of cameras to other security elements. This connection allows the synchronization of the cameras' recordings and the events of devices. This enables faster and better responses to any critical situation.

It is not necessary for operators to have an in-depth understanding of the security system or its devices. ATS8600 controls and manages these devices within the unified user environment. It enables not only a short implementation period, but also a timely staff training.

Authorized company and security company employees do not have to deal with the details of how these devices work, which allows them to focus on their duties. They can focus on a more efficient operation management of individual devices and improve security.

ATS8600 system can only distribute information that is within the assigned aspects of the system to trusted employees, which significantly reduces the risk of information misuse.

The availability of some functionalities described in this User guide may vary according to the application edition.

1.2 Technical specifications

The technical specifications define the technical parameters of hardware equipment concerning the server and workstations.

Technical specification of the server for ATS8600 server

Configuration for smaller installations:

- 1 GHz processor or faster
- HDD: 60 GB
- RAM: 2 GB
- OS: Windows 7 or Windows 8 (except for Starter and Home editions)
- Database: MS SQL 2008, MS SQL 2012, MS SQL 2014 (Express or Standard edition)

Configuration for medium-sized installations:

- 2 GHz processor or faster
- HDD: 60 GB
- RAM: 4 GB
- OS: Windows Server 2008, Windows Server 2012
- Database: MS SQL 2008, MS SQL 2012, MS SQL 2014 (Standard edition)

Configuration for larger installations:

- 2 x 2 GHz 32-bit (x86) or 64-bit (x64) processor
- HDD: 2 x 60 GB (RAID 1)
- RAM: 8 GB
- OS: Windows Server 2008, Windows Server 2012
- Database: MS SQL 2008, MS SQL 2012, MS SQL 2014 (Standard edition)

Note:

To use MS SQL Standard edition with ATS8600, at least 3 CAL licenses are required:

- one CAL license for Internet Information Services
- one CAL license for ATS8600 system services
- at least one CAL license for ATS8600 application user

Technical specifications of the ATS8600 Client PC

Any PC meeting the requirements for running Windows XP Professional SP 2 or higher:

- Pentium - 1.5 GHz or faster
- HDD: 20 GB
- RAM: 1 GB
- Available connection to ATS8600 server

Note:

If camera system video is displayed on the ATS8600 client station, hardware requirements of the camera system for video viewing are to be considered as well.

1.3 Security of Integrated Security Management System

The security of the system prevents unauthorised access to the data stored on the server.

Security on the server level

Communication between the server and the workstation PC is provided by transparent http and https protocols. All user permissions and access rights are set up, controlled and verified on the level of the ATS8600 central server. Any change or operation performed by operators is saved and stored for later evaluation. All administrator operations within the database are automatically recorded for later evaluation.

Security on the level of the workstation PC

A client PC with ATS8600 application does not allow unauthorised access to data, as the computer operating the ATS8600 client operating computer does not store any data on local media.

Security of communication between the workstation PC and the server

The workstation PC and the server communicate exclusively through http protocol or, for higher security, through secured SSL connection. This ensures the security level of internet banking applications.

Communication security between the server and devices

Because the device manufacturer communication protocol is not always encrypted, the server-device communication security and protection is performed at the network administration level. Protection on the level of net administration can be provided by encrypting (VLAN).

Personal data protection

Application user access to personal data stored in system database is governed by the terms of the personal data protection act.

2 Operating procedures

2.1 Integrated Security Management System start-up

The application starts after selecting a command to start (e.g., by selecting an application from the Start menu through Programs -> UTC Fire & Security -> ATS8600 Client). Each user logs in with their user name and password. Without this, access to the application will be denied.

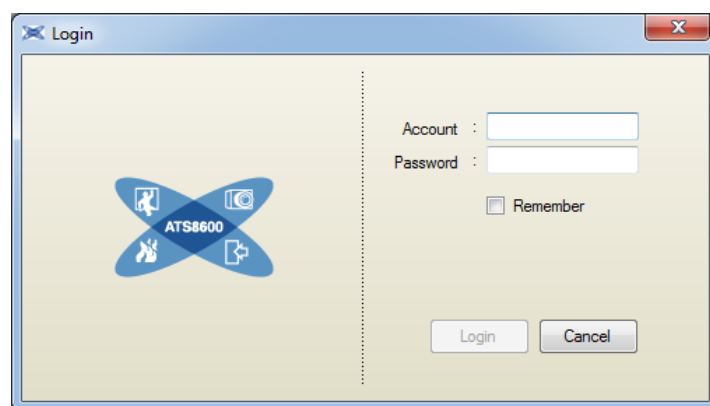


Figure 2-1 User login to the system

In the login window, enter the appropriate information:

- *Account* - user login name
- *Password* - password in accordance with the company's security policy

In this login window you can also choose other attributes for logging in to the application by checking the relevant boxes.

- *Remember* - after checking this box, the system will remember your login data, which will appear automatically in the login window next time you run the application.

The language of the login window is always the same as the language set in Windows.

The language in the remainder of the application is set by default to English. The language can be changed. Click *Tools, Settings, Personal Settings* ([see chapter Personal Settings](#)).

2.2 Structure of the Professional panel

After a successful user login to the system, the main screen of the application will be displayed. Depending on the settings for the particular person, this may be the Professional view as shown below, but this may also be the Visitor view or the Monitor view.

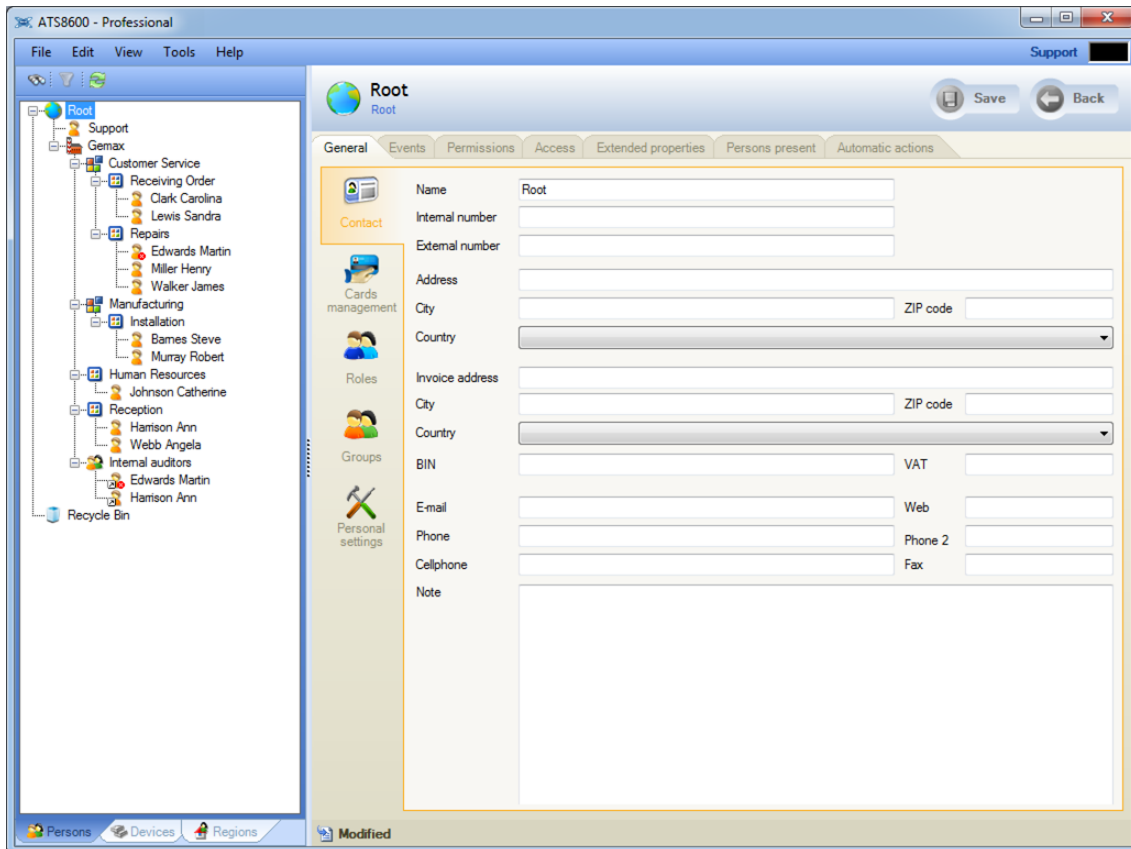


Figure 2-2 Professional window

2.2.1 Main menu

The Main Menu contains the commands for general system functions and links to every other application part:

- **File** - contains the list of functions available at your current location in the application. You can usually select each function in several ways (e.g. right-click).
- **Edit** - allows some modifications when working with the system (e.g., **Back**, **Refresh**, **Find**).
- **View** - contains panels (depending on the system version) for:
 - viewing persons, devices, regions, manage visits
 - view the visualizing representation of devices in maps,
- **Tools** - contains panels for:
 - defining the system settings for the application (personal settings, password change, system settings),
 - designing the visualizing representation of devices in maps,
 - manage assets,
 - set the data import from external information system.
- **Help** - general information on the ATS8600 System, user handbook and information on licenses ([see chapter Licensing](#)).

Hotkeys are shown next to the respective individual menu items. These can be used to intuitively perform common operations in the application (e.g., **Find**, **Refresh**, **Delete**, etc.).

2.2.1.1 System restart

The File option in the Main Menu contains a restart function for ATS8600 system restart. The system will end and a login window appears. It is used for a quick re-login of the user to apply system changes. Clicking **Exit** will end the system's session.

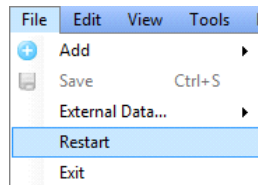


Figure 2-3 Application restart

2.2.2 Tree

The tree, with its node and child-nodes, provides for a graphic representation of elements for easy navigation and application-to-user communication, as it enables the presentation of complicated data structures in an easy and comprehensive way. It allows instant data searches in the hierarchical system structure. It is displayed on the left side of the screen.

Note:

A node is the highest element in the tree but below the root node. It is also referred to as parent node. Children or child-nodes are sub-nodes under a (parent) node. As an example: the company is a (parent) node. A department is a child node of the company (resides under the company).

2.2.2.1 The tree tab

The tree tab is a graphical shortcut for the tree option: *Persons*, *Devices* and *Regions*. In the lower left corner, the active tab is highlighted with a different colour than the inactive tab.

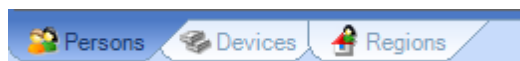


Figure 2-4 Tree tabs

2.2.3 Toolbar

This contains tools that can be used whenever and wherever you are working with the tree.



Figure 2-5 Toolbar

- **Search**
Allows searching of the given tree. A detailed description of how to search is included [in chapter Search](#). You can find **Search** in *Edit* as well.
- **Filter**
A tool for filtering devices with a given status.
- **Refresh**
Clicking this function will revert the tree to its last saved state.
- **Statuses on**

This function is located in the Devices and Regions tree ([see chapter Device statuses](#)). Devices statuses are displayed.

- **Devices**

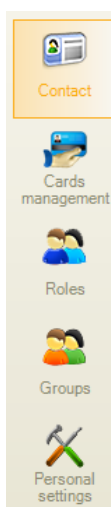
This function is located in the Regions tree ([see chapter Regions](#)). Makes it possible to distribute devices into regions.

- **Print**

After turning the filter on, this function makes it possible to print elements matching the selected filter criteria.

In different views, some additional tools are available. Details are explained in the relevant section.

2.2.4 Infotypes Panel and its tabs



The Infotypes panel includes the following tabs:

- **Contact** - the main view of the selected tree node. Contains the name of the node with basic details and contact data.
- **Card Management (Credentials)** - list of cards or credentials allocated to the selected group (card management) or a person (credentials). A credential is a unique element used for identification of a specific person.
- **Roles** - it is possible to assign a set of pre-defined permissions to users according to typical tasks performed.
- **Groups** - list of defined groups in the tree.
- **Personal Settings** - application related settings of a particular user (including application password and account).

Figure 2-6
Infotypes panel

2.2.5 Navigation Panel and its tabs

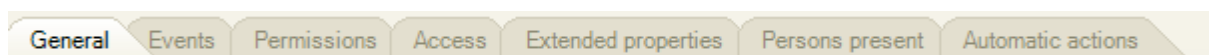


Figure 2-7 Navigation panel

The navigation panels of the *Persons* and the *Devices* tree are similar. They contain the following tabs:

- **General** - this tab provides basic information on the selected information system object. This tab contains the tabs of infotypes: *Contact*, *Credentials*, *Roles*, *Groups*, *Personal Settings*.
- **Events** - the list of all performed activities and changes including the time and the description of the change. The events can be displayed only for the selected persons or device, or including all persons in a company or department. To reduce the number of events, it can be restricted by filter or by time period ([see also chapter Events](#)).
- **Permissions** - this tab presents an overview of persons' access rights to specific system objects (devices, persons, events, application parts). The permission system is based on the principle of inheritance from a parent to its descendant ([see chapter Example of configuring permissions](#)).

- *Access* - this is one of the subcategories of the previous *Permissions* tab and it provides a comprehensive overview of which persons have access to specific devices. In *Persons* this shows the selected group or persons access. In *Devices* it provides a list of persons and access rights to the selected device ([see chapter Access rights](#)).
- *Extended properties* - settings of additional and specific properties of the object.
- *Persons present* - this tab provides information about the location of the person selected in the organizational structure. By selecting a company (division, department, center), you can display all regions that contain the persons belonging to the selected organizational structure. Person-counting set-up is described [in chapter Number of persons in the region](#).
- *Automatic actions* - provides an overview of automatically launched actions, when a predefined action set by a user occurs on the device ([see chapter Automatic actions](#)).

2.2.6 System information

This is recorded and displayed automatically by the system and cannot be edited by the user. This provides information about the user and time of the last change of the object where the user is currently located.

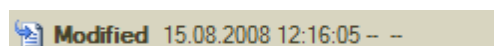


Figure 2-8 System information

2.2.7 RT status (Real-Time system heartbeat)

RT control is a function for connection diagnostics between ATS8600 client and the server. The status of the connection is indicated by an icon in the upper-right corner of the application.



Figure 2-9 RT Status

In the basic setting, this icon is black . In this case, it does not display connection status correctly. When status monitoring is enabled ([see chapter Toolbar](#)), it can have the following colours:

-  - a green ECG signals an ongoing communication between the server and the client.
-  - a red flat ECG signals a non-existent connection between the server and the client.

If the connection is lost, the user is notified by a sound.

2.3 Working in the Professional view

2.3.1 Working with the tree

The tree, with its nodes, is the main information view for any user as it enables a quick overview of even complicated data structures. It allows for quick selection of objects present in the tree. Selecting a node in the tree (object) displays its details on the right-hand side of the screen. The top of both the *Persons* and *Devices* trees consists of the *Root* node, the data of which can be

edited only in accordance with the access permission. Without access permission the right-hand side application window is greyed out. However, you can create hierarchical tree structure from this node.

Manipulation with the Tree

To expand or to collapse the node use the following controls:

"+" expand (show parent and children of this parent)

"-" collapse (show parent only)

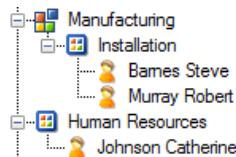


Figure 2-10 Expand and collapse controls

The following keyboard shortcuts can be used when working with the tree structure:

- expanding the selected node showing children of this node only: NUM+
- expanding the selected node, including all child nodes underneath: NUM*
- collapsing the selected node: NUM-

If the tree window is not wide enough to fit all the data, the user can adjust the width of the tree window by moving its edge using the mouse. Also, when positioning the mouse over the specific name, the full node name is displayed. Another option is to enlarge or maximize the entire application window.



Figure 2-11 Moving the split bar

Press **CTRL+X** to cut the currently selected object and put it to the Clipboard. The Clipboard content can be pasted to another part of the same tree. Select the node in the tree, under which the object from the Clipboard should be pasted, and press **CTRL+V**. The object will be moved including its child nodes. The object currently in the Clipboard is greyed out in the tree. Moving objects using keyboard shortcuts is supported in *Persons*, *Devices* and *Regions* trees. The object can be pasted only under a node, under which it is possible to create the type of the moved object using the Add function as well. After the object is successfully moved Clipboard is emptied and the object will have its usual graphics. In case of an attempt to insert the object to an unsupported location, Clipboard will be emptied and the operation will be terminated without any change in the tree structure.

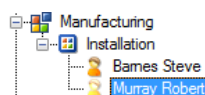


Figure 2-12
Object in
Clipboard

2.3.2 Confirming and saving changes

The normal procedure to confirm or cancel changes is by using the **Save** and **Back** buttons. Clicking **Save** will save all changes made by the user. If a problem while saving occurs (e.g., some required data is left blank), the system prompts the user to fix the problem.



Figure 2-13 Save and Back buttons

Other unexpected problems can occur during saving (e.g., connection failure). If the problems continue, contact your system administrator.

If you want to revert the system into the previously saved state, click **Back**.

Greyed out buttons mean that the data was not changed, so there is nothing to revert to the previous state.

In cases when two or more users perform changes to the same object and save them almost simultaneously, changes from both sources will be saved to the vent list, although only the last saved change will take effect.

The performed operation can be reverted back only if the changes are not saved. When working in one application section (e.g., in one node), several operations can be performed and multiple amounts of data can be saved without having to click **Save** each time. When moving to another section, the system will prompt you to save the changes.

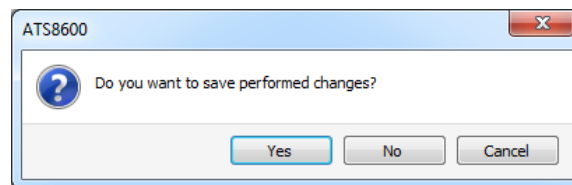


Figure 2-14 Dialogue box

2.3.3 Function selection in the tree

The functions for objects in the tree can be selected using the **File** menu located in the main application menu, or by right-clicking and using the context menu.

To perform a function of the object, click on this object to highlight it and then right-click it. The list of available functions will pop up.

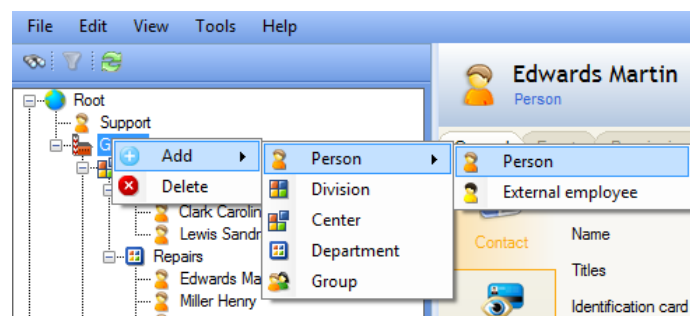


Figure 2-15 Selecting a function

You can find the same list of available functions that can be selected for the specific object in the *File* menu.

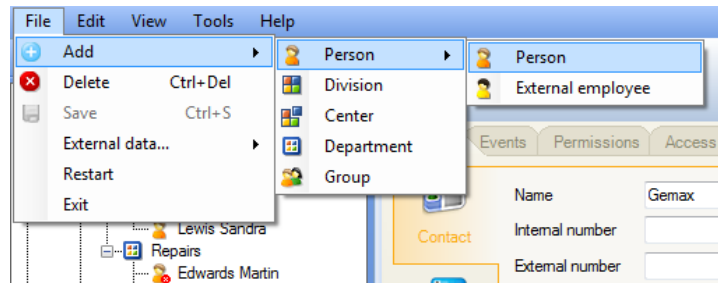


Figure 2-16 Selecting a function from the File menu

2.3.4 Search

Click  , a search bar opens that can be used to search for items in the tree.

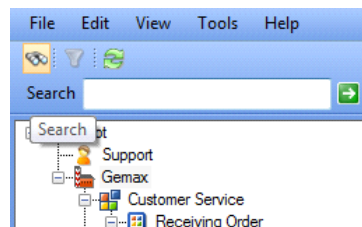


Figure 2-17 Launching the search bar

The search bar makes it possible to define a number of search criteria to optimize the search process. The criteria must have the following form Key:Value Key2:Value2 Individual conditions are separated by a space.

You can search for all items from the *Persons* tree listed in the *Contact* tab (except for *External number*). It is also possible to search according to identifier parameters.

The *Devices* and *Regions* trees can be searched using the *Name* key.

Example:

In the organisational structure of a company we search for a person called Edwards with the internal number 1200048. Enter the following criteria into the search bar: Surname:Edwards "Internal number":1200048

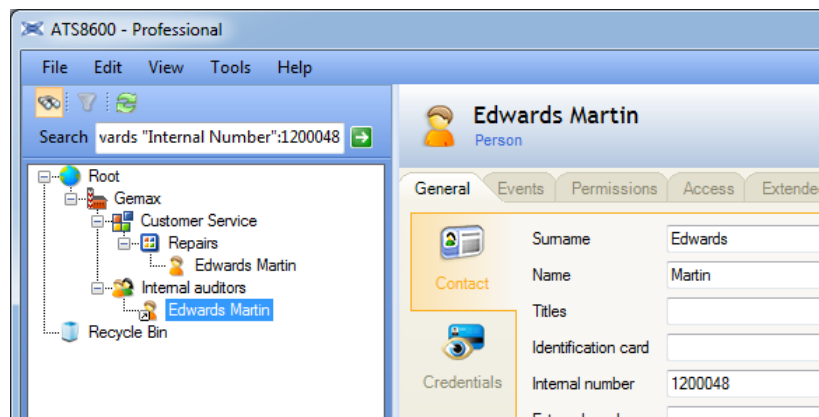


Figure 2-18 Search using the surname and internal number

Clicking  will start the search. The system displays only those results that meet all entered search criteria and the parent structures that are necessary to maintain clarity. After changing the search criteria, click  again to update the search results.

Note:

Search conditions are not case sensitive. This means that the condition Surname:Edwards is equivalent to surname:edwards.

Warning:

If the search key or the search value contains a space, you need to use quotation marks. For example, City:"New York" "Internal number":1200048.

Tip:

Search keys that contain spaces can be used without them. Condition "Internal number":1200048 can thus be replaced by an equal condition Internalnumber:1200048 (in such cases quotation marks are not required).

Entering the searched value without a search key performs search in all supported items.

You can search persons based on their legitimacy, which is determined by entering the start and end date of their employment. This status is defined by search key Disabled and can have two values: True (the person has been denied access to the ATS8600 system) or False (the person can access the ATS8600 system).

In case of credentials, you can search the following properties:

- *Credential name* - search key *Name*
- *Credential status* (active, blocked, lost) - search key *Status*
- *Credential code* (only in case the credential type supports search or the user has the Viewing PINs rights) - search key *Code*

3 User management

The *Persons* tree is intended for management of the company's organizational structure. The ATS8600 Integrated Security Management System makes it possible to manage the persons register using the organizational structure, assign individual credentials to them (cards, PIN, fingerprints, eye iris images) and define permissions for these persons.

3.1 Entering start date and end date of access

When a new person is employed, you can set a date interval when the person will be able to access the system by entering details in the *Contact* tab. Outside of this interval, the person will not be able to access anything or login. A person who is outside the assigned date interval is marked with a cross in the *Persons* tree.

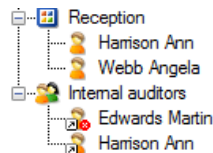


Figure 3-1 Person outside the allowed date

Date formats depend on the set language of the ATS8600 application user.

Example:

English (US) - 12/31/2010

German - 12.31.2010

Slovak 21. 31. 2010

Edwards Martin
Person

Save Back

General Events Permissions Access Extended properties Persons present Automatic actions

Contact

Credentials

Roles

Groups

Surname: Edwards
Name: Martin
Titles:
Identification card:
Internal number: 1200048
External number:
E-mail: edwards@gemax.com
Function:
Sex: Male
Valid from: 01/01/2010
Valid to: 01/01/2013
Address:
City:
ZIP code:

Figure 3-2 Setting the start and end date for a person

Note:

If the date format is not valid and recognized, the user cannot leave the field. It is not mandatory to enter a start and end dates.

3.2 Creating the organizational structure

The Organizational Structure (OS) of the company is created by adding individual objects and records to the *Persons* tree.

The initial point of the navigation tree within the OS creation is the *Root* node. Using the **Add** function, new objects of the following types can be created from this node:

- Company
- Group
- Person

A user with sufficient permissions to create the OS may proceed as follows.

3.2.1 Adding the company to the OS

1. Right-click the *Root* node and select the **Add - Company** pop-up menu command.

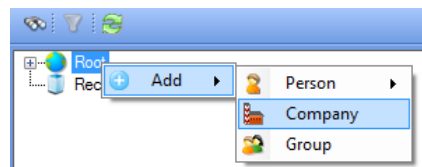


Figure 3-3 Adding a new company

2. Selecting this function activates the dialogue box for entering the company name on the right-hand side of the screen. After entering the name, confirm by clicking the **Save** icon in the upper right-hand corner of the screen.

A screenshot of the 'Contact' dialogue box in the 'Gemax' application. The window has a title bar with 'Gemax Company' and 'Save' and 'Back' buttons. Below the title bar are tabs for 'General', 'Events', 'Permissions', 'Access', 'Extended properties', 'Persons present', and 'Automatic actions'. The 'General' tab is active. On the left is a sidebar with icons for 'Contact', 'Cards management', 'Roles', 'Groups', and 'Personal settings'. The main area contains a form with the following fields: 'Name' (filled with 'Gemax'), 'Internal number', 'External number', 'Address', 'City', 'ZIP code', 'Country' (dropdown menu showing 'United Kingdom'), 'Invoice address', 'City', 'ZIP code', 'Country' (dropdown menu showing 'United Kingdom'), 'BIN', 'VAT', 'E-mail', 'Web', 'Phone', 'Phone 2', 'Mobile phone', 'Fax', and 'Note'.

Figure 3-4 Contact dialogue box

3. The system will alert you if any required fields are left empty. Please enter proper details in the required fields.

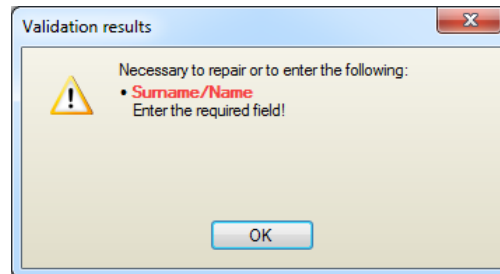


Figure 3-5 System warning

4. Click **Save** in the upper-right corner of the screen.

At the level of the Company tree node, the administrator of the OS can create the following types of objects using the **Add** function:

- Person
- Division
- Center
- Department
- Group

3.2.2 Adding a department to the OS

The department, as an element of the company organizational structure, can be created by clicking the Company tree node for which you wish to create the department. Right-click the item and select **Add -> Department** from the menu.

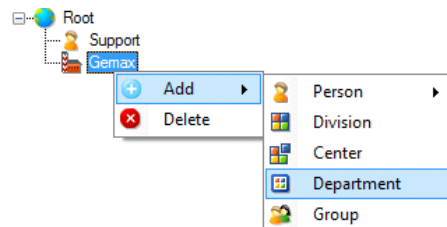


Figure 3-6 Adding a department

When entering the contact information of the department into the *Contact* dialogue box, proceed as described [in chapter Adding the company to the OS](#).

3.2.3 Adding other types of record to the OS

The method for adding other types of records (division, center, person) to the company's OS is similar to that as adding a company as explained before ([Adding the company to the OS](#), [Adding a department to the OS](#)).

A record cannot be placed at random. The system contains a controlled support for hierarchies; that is, the system controls what type of record can be created at any given node of the navigation tree. This will be apparent in the function menu when creating a new record.

The system enables the creation of several companies in the tree. When creating persons in individual companies, one person may not be assigned to two or more companies. The system does not support

this functionality. However, any person can be transferred between companies or OS elements.

3.2.4 Changing an OS record

Any record in the OS structure can be modified. Select the record to change and choose the detail to be modified in the dialogue box. The dialogue box is displayed in the editing status. This means that information in this dialogue box can be changed before saving. To copy and insert selected text or part of the text, the standard windows shortcuts may also be used: *Ctrl+C* and *Ctrl+V*.

Address	37th Street 152/5
City	Toronto

Figure 3-7 Editing a record

To save any change, click the **Save** button. The changes will not be saved by clicking the **Back** button.

3.2.5 Importing the Image to the Person's Record

When adding a person to the system, by entering details in the *Contact* tab, it is also possible to add a picture of that person.

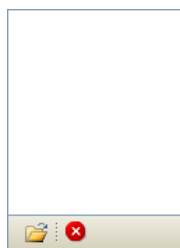


Figure 3-8 Window for a person's picture

Add the picture by clicking the  button and select the required image in any folder. Supported image formats of photos: *.png, *.jpg, *.bmp. To delete the picture, select the  button.

3.2.6 Deleting the Record

To delete a record from the structure in the navigation tree (organizational structure), right-click the node representing the record and select delete.

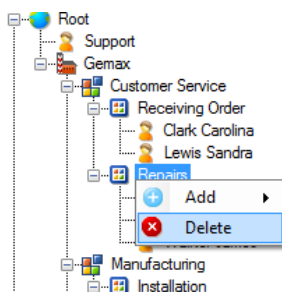


Figure 3-9 Deleting an object

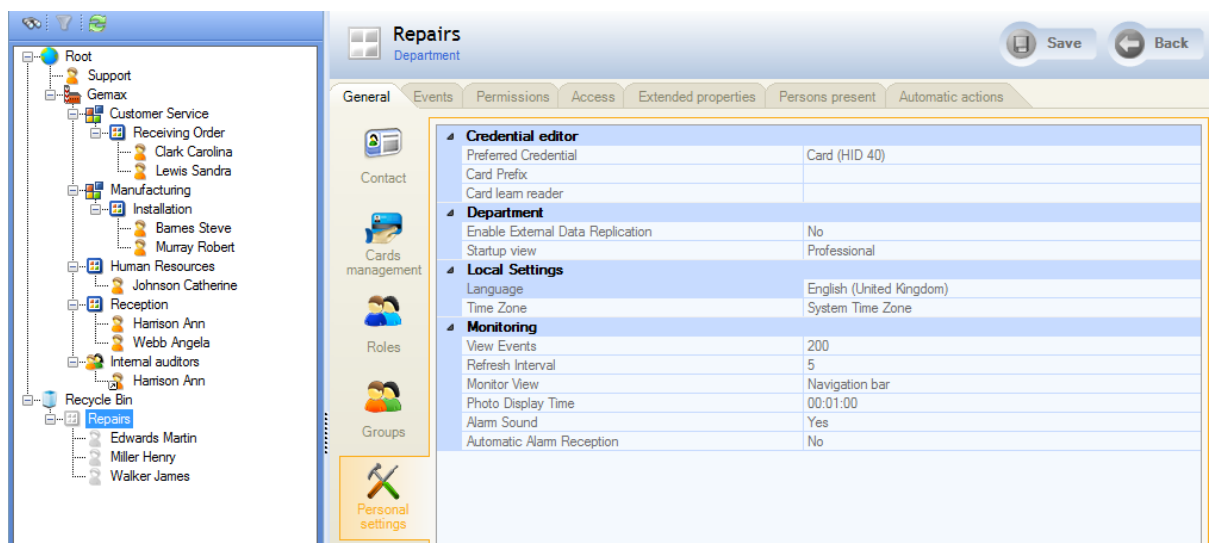


Figure 3-10 Deleting an object

Click **Delete** to move the object into the recycle bin.

Objects in the Recycle Bin are characterized as follows:

- Objects in the Recycle Bin are greyed out.
- The structure of the deleted part of the tree is also kept within the Recycle Bin.
- In case of the next upload, persons will not be uploaded to the devices. Their ATS8600 accounts will be blocked too.
- You can search the object event history.
- Editing objects is disabled.
- Changing the object structure is disabled.
- The contents of the Recycle Bin cannot be exported or imported.

Note:

The Recycle Bin is available only in the *Persons tree*.

Warning:

Groups from the *Persons tree* are deleted permanently and are not moved into the Recycle Bin.

Restoring the objects in the Recycle Bin

In order to preserve the tree structure, the only items that can be restored from the Recycle Bin are those whose parent has not been deleted (its original parent items exists in the tree). Right-click the *Repairs* department and then click **Restore**. The *Repairs* department receives its original place in the organizational structure.

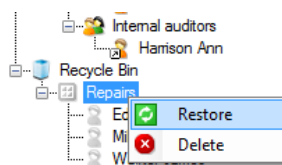


Figure 3-11 Adding a department

Right-click the Recycle Bin and click **Restore all items** to restore all items.

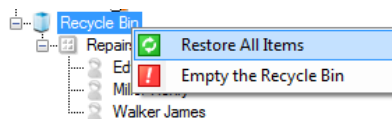


Figure 3-12 Deleting an object

This operation has to be confirmed in the dialog box.

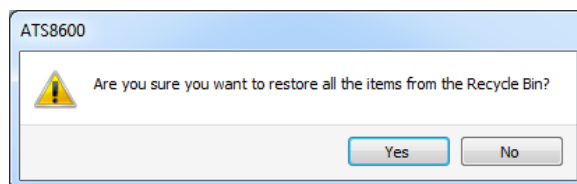


Figure 3-13 Confirming the restoration of all items in the recycle bin

Deleting items from the Recycle Bin

To delete an item from the Recycle Bin, right-click the item and choose **Delete**. If you delete an object from the Recycle Bin, its history is also deleted permanently.

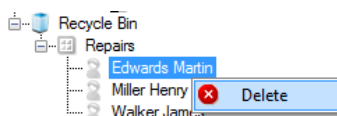


Figure 3-14 Deleting a record from the Integrated Security Management System permanently

To empty the Recycle Bin, right-click the bin and choose **Empty the Recycle Bin**. In the dialog box, confirm that you want to delete all items from the Recycle Bin permanently.

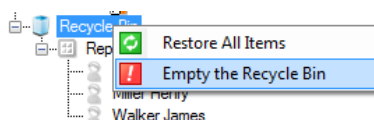


Figure 3-15 Emptying the Recycle Bin

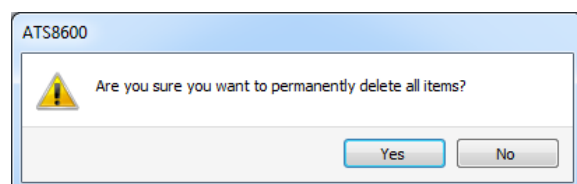


Figure 3-16 Confirming that you want to delete all items from the Recycle Bin permanently

Warning:

If the OS record is listed in one of the groups ([see chapter Group management in the OS](#)), **Delete** will

also delete the record from the group where this record is listed.

Note:

If you select an object in the tree using *Shift+Delete*, the object will be deleted permanently without being moved to the Recycle Bin. Since this operation cannot be reversed, we recommend using it only if necessary.

3.2.7 Group management in the OS

In the *Persons* tree you can create groups under the *Root* or *Company* nodes. These are organizational elements that can include representatives from various parts of the organization.

The purpose of groups is to enable permissions to be assigned to records (e.g., administrators of multiple departments may have their own group, which will assign permissions for the application). Permissions inherited from groups are taken into account in the calculation of the final permission together with assigned roles and individual permission settings.

3.2.7.1 Creating the group

You can create a new group by right-clicking the *Root* or the *Company* node in the tree and selecting *Add - Group*.

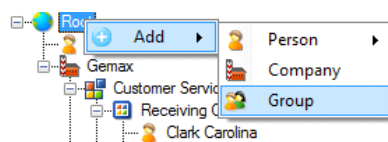


Figure 3-17 Creating a new group

The dialogue box for entering information about the group is shown at the right-hand side of the screen. Follow the steps [in chapter Adding the company to the OS](#).

3.2.7.2 Adding an Object into a Group

Warning:

It is not possible to create new records in a group. Use drag & drop to add a previously created record (within the OS) to the group:

1. Left-click node representing the required node record in the tree (company, department, division, centre, person) you want to add to the group. A group cannot be added to another group.
2. Hold the mouse button and move the object to the desired group. The mouse pointer will change its shape while moving.
3. Release the button when the pointer is placed over the group name and the mark "☞" will be displayed next to the pointer.

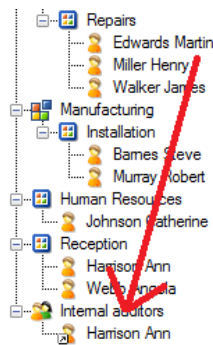


Figure 3-18 Moving a person into a group

4. The person is assigned into the group:

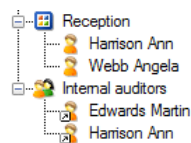


Figure 3-19 Records listed in the group

Warning:

Each person must be moved individually. It is not possible to move more than one person at a time.

Similarly, you can add the person into the group after clicking the *Groups* infotype.

1. Select the person you want to add to the group in the Persons tree.
2. Click the *Groups* infotype. All defined groups to which the selected person is to be added are displayed at the right-hand side of the screen.
3. To add the person to the group, check the box next to the name of the group. This method is similar to those mentioned above (drag & drop).

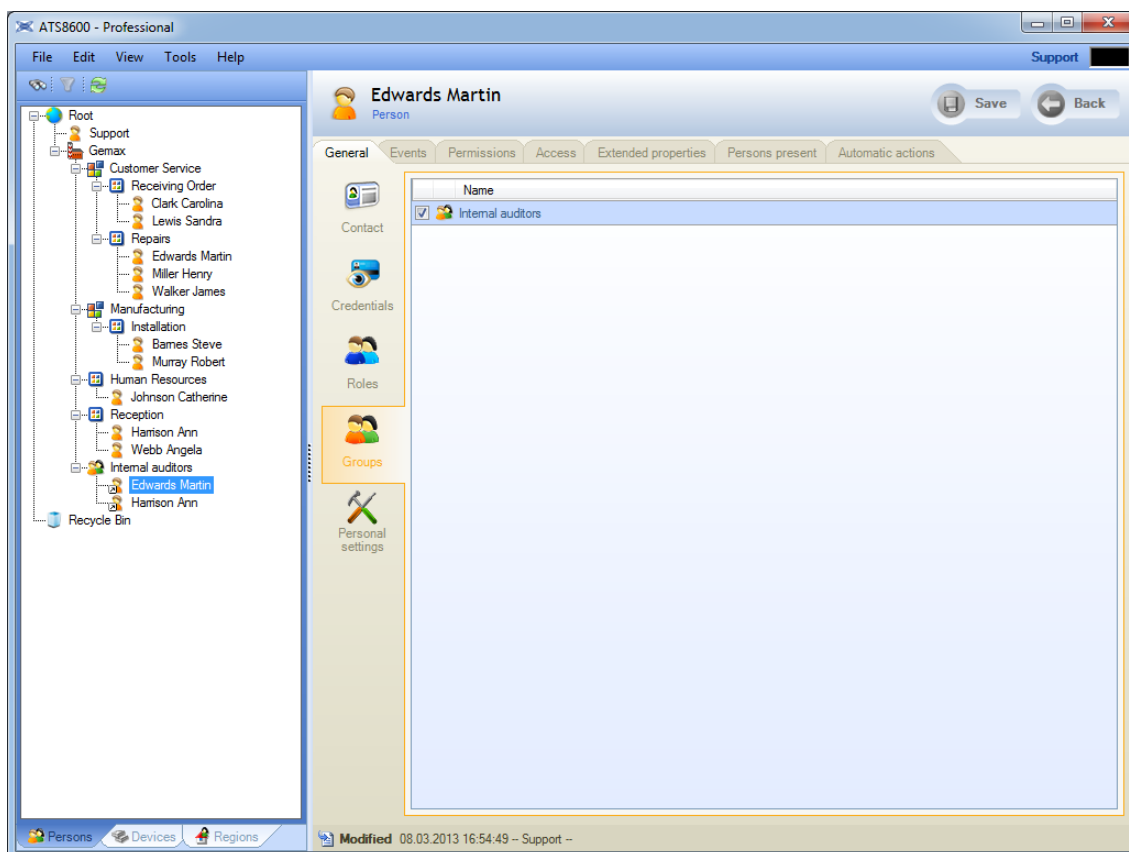


Figure 3-20 Groups infotype

The view of the *Groups* infotype provides an overview of groups that are defined within the tree and groups to which the selected person is added.

3.2.7.3 Removing an Object from a Group

As it is not possible to create records in the group (only to move them into a group), it is also not possible to delete a record from the group, only to remove it.

If you want to remove a person from a group, right-click the person and choose **Remove**.

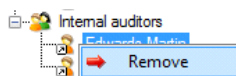


Figure 3-21 Removing a record from a group

If you do not save your work when moving to another section, the system will prompt you to save the changes. Another way to remove a person from a group is to select the person in the tree and uncheck the box in front of the group name in *Groups* infotype.

3.3 Credentials Management in OS Environment

A credential is a unique element used to identify a person in the company's OS. Each credential is assigned to a particular record (usually to a person). Credentials are managed in the tab of the respective infotype of the *Infotypes* panel.

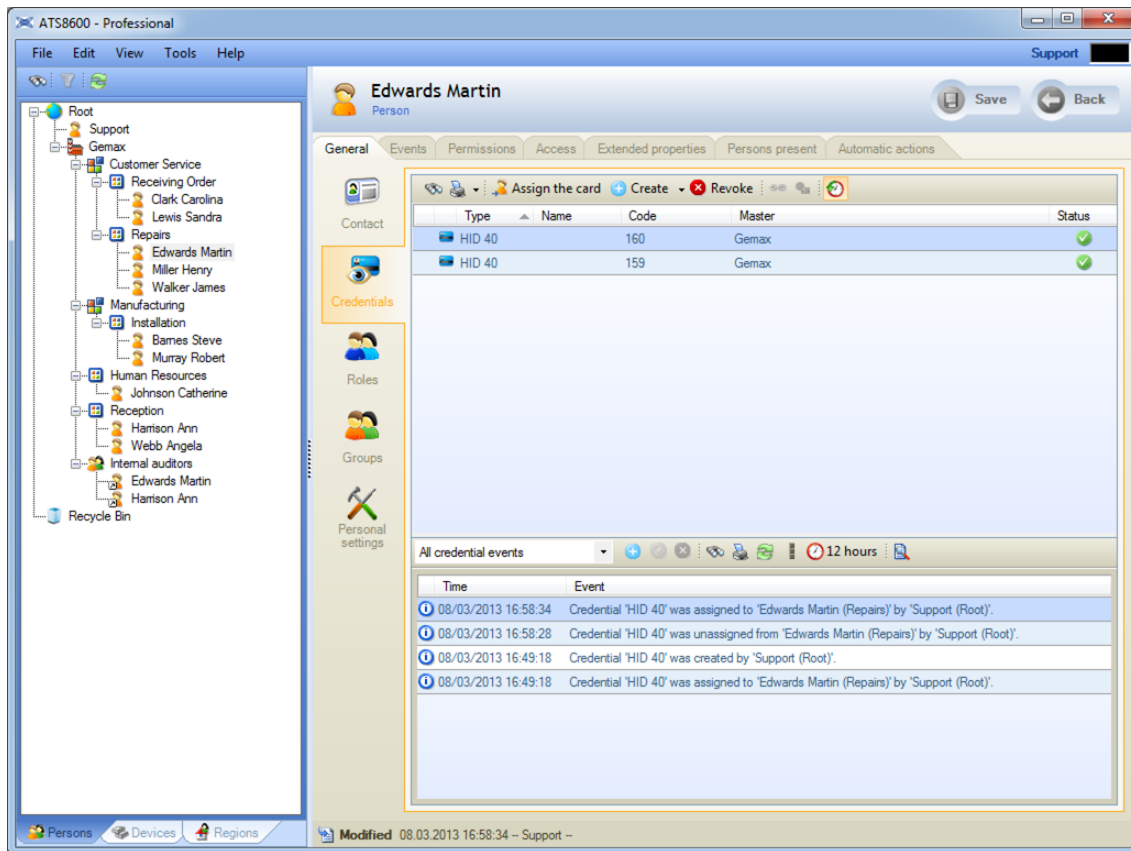


Figure 3-22 Credentials dialogue box

3.3.1 Types of credentials

The access control system uses five types of credentials:

- *PIN* - numerical code entered on a keypad. For security reasons, PIN codes are not shown (e.g.: ****). Two persons cannot have the same PIN at the same time.
- *Extending PIN* - numerical code entered on a keypad. It can be used in the system only in combination with another credential type (e.g., a card). Since the extended PIN is a code combined with other credential type, two people can use the same extended PIN, but each must be in combination with a different credential. Extended PIN, entered into credentials management, can also be a *. In that case, after using a card paired with such an extended PIN, the user will be prompted to use the keypad of the device and set the extended PIN (this function must be supported by the device).
- *Card* - identification element, plastic card containing the data from the card
- *Iris* - biometric details - human eye
- *Fingerprint* - biometric details - fingerprint

As for the person's property right, the credentials are classified as:

1. The private credential is an identification element that is non-transferable to another person. It is called a private credential due to the fact that the person is the carrier of the data. Private credentials can be created and deleted but not removed and assigned to

another person.

- Iris
- Fingerprint
- PIN
- Extending PIN

2. The shared credential is a transferable credential. It can be used by another person, or can be removed from the person and assigned to another one.
 - Card

3.3.2 Card Management

Cards are a type of credential assigned to a particular object. In the case of cards - shared credentials - the system differentiates between:

1. *Card Master* - the company, department or division that manages the card and decides on cards assignments to persons that are included in the respective company, department or division within the organizational structure.
2. *Card Holder* - person to whom the card is assigned.

The list of cards and the holder or not yet assigned cards can be seen in the *Card Management* tab. A new card can be created by clicking the **Create** button. Creating a card for an OS unit is described [in chapter Creating a card](#). Information about the last change of the card can be found in the bottom line of the application window as the system information (date and time of the change and the user who performed it).

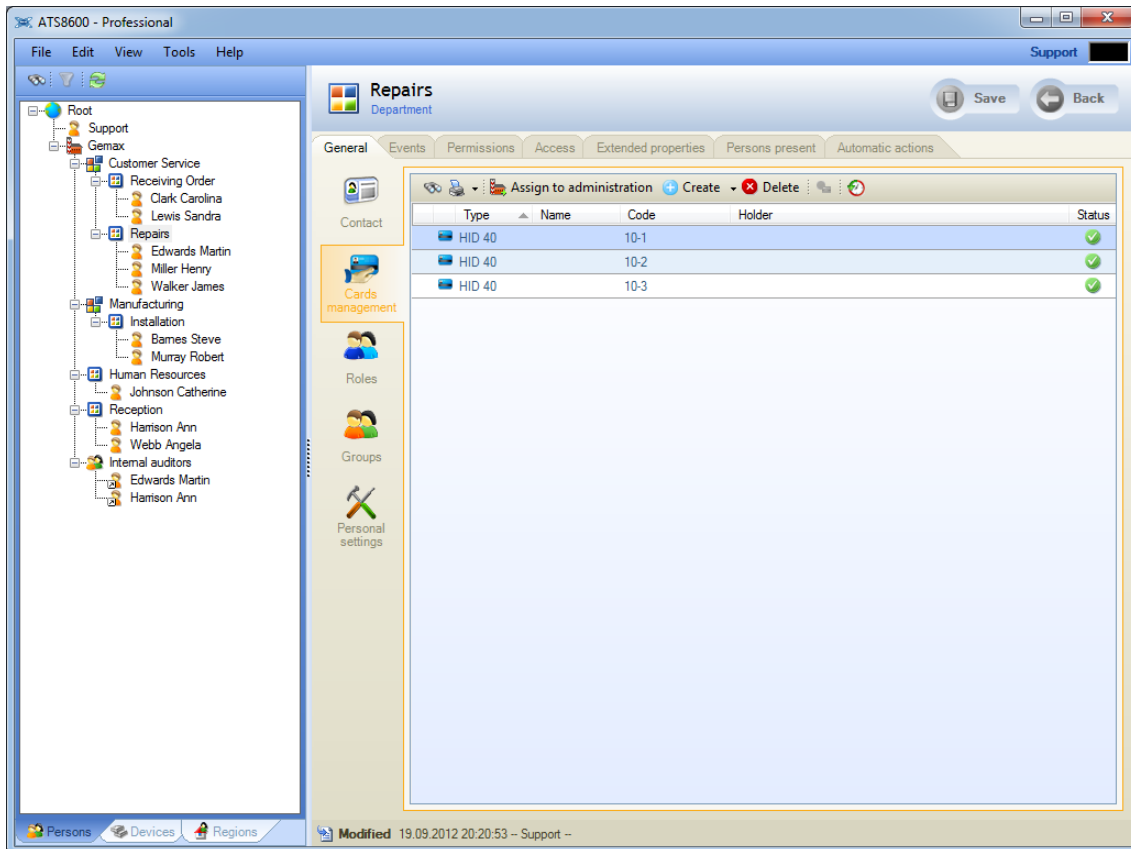


Figure 3-23 Free credentials managed by the Repairs department

Sorting the list

The card list can be sorted by any column. By clicking the column header, the list will re-order and a triangle will appear in that column to indicate ascending or descending order.

Type	Name	Code	Master
Ats lum 26		3018080	Gemax
Ats lum 26		0138080	Gemax
HID 40		159	Gemax
HID 40		160	Gemax

Figure 3-24 Sorting the cards by type in ascending order

Printing the list of credentials

The function of printing the list of credentials is shown on the figure below. The list of credentials includes all properties of credentials, including their status.

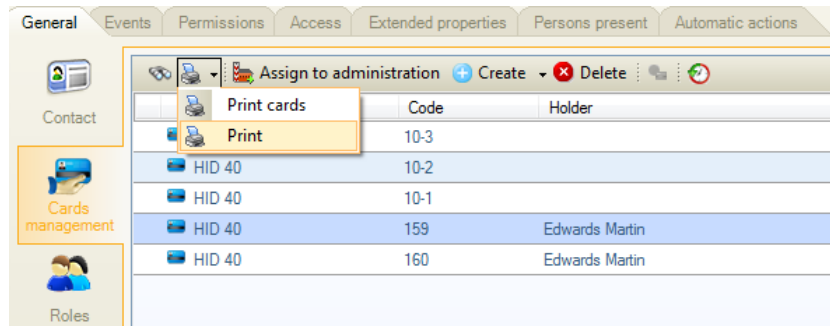


Figure 3-25 Printing the list of cards

Printing cards

The Print cards function makes it possible to print cards assigned to persons. This function is used to print on cards of individual companies and it makes it possible to use a unique graphical design created according to the requirements of the particular user. A graphical design belonging to the respective part of the organizational structure can be uploaded by clicking  and selecting a RDLC file in the dialog box. For a more detailed procedure of editing RDLC files see the Card Imprint Design guide.

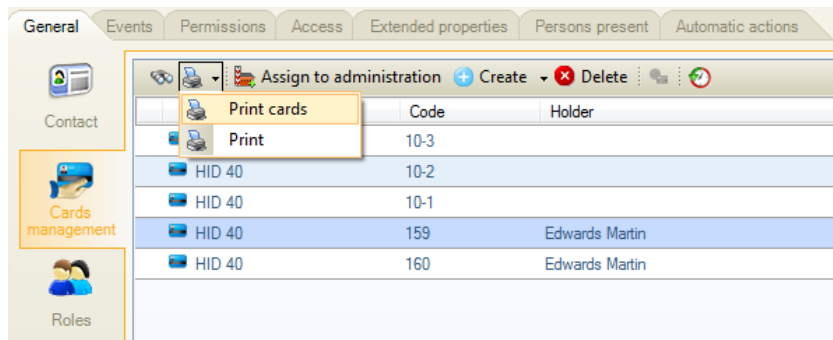


Figure 3-26 Function for printing cards

However, only records selected via multiselect (i.e., holding the *Ctrl* key and clicking individual records or holding *Shift* and clicking the first and last record) will be printed.

3.3.3 Assign to administration

Cards managed by an element of the organizational structure are searchable. Click **Assign to administration**. The window appears. Enter the code or card name (or the part thereof) you want to search for into the *Code* field. The system will search for all cards that are managed by the specified unit of the organisational structure.

Clicking  without filling the *Code* field displays the list of all credentials in the Persons tree.

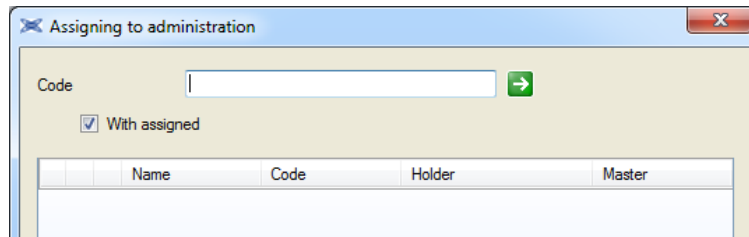


Figure 3-27 Card search window

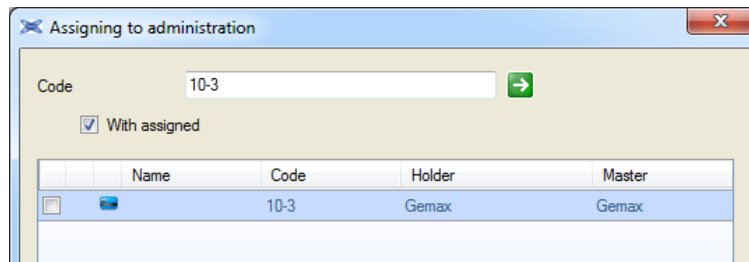


Figure 3-28 Found card

The found cards in the search list window can be sorted by any column as shown on figure below. This enables you to find the required card faster.

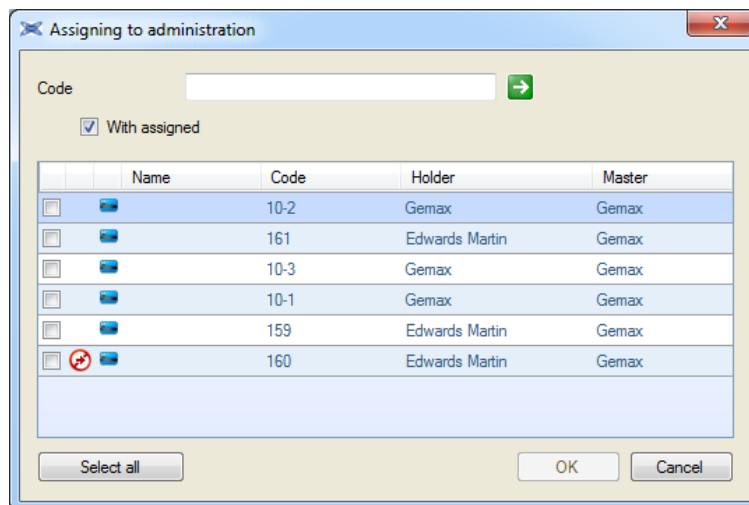


Figure 3-29 List of all credentials that are managed by company, division or department

To see which card is assigned to an actual person, click the name of the person in the tree and open the Credentials tab on the right-hand side of the screen. The list of credentials assigned to the person and other information is displayed.

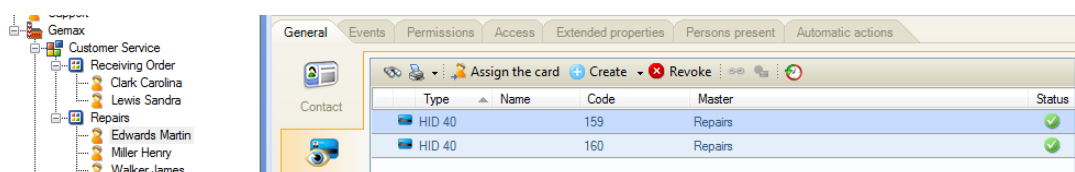


Figure 3-30 Credentials view

3.3.4 Creating a card

Cards are added for companies, departments, or divisions from the list of cards supported by the application:

1. In the *Persons* tree, select the company, department or division for which you want to create the card. In the *Card Management* tab click **Create** to select the required card type.

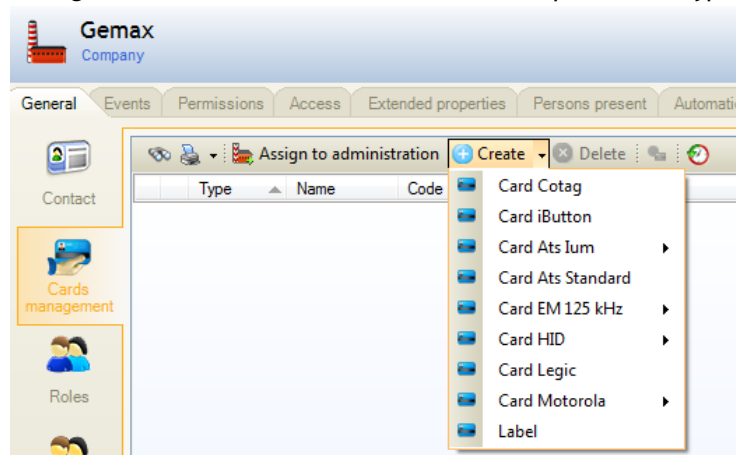


Figure 3-31 Creating a card

2. The selected card is entered into the list (or added to the list of cards not assigned to any person).
3. Enter other information: name, code and card status. The majority of these fields are required:
 - *Name* - name for the credential (optional field)
 - *Code* - the card number as provided by the device using letters, numerals, characters (code on the card) (mandatory field).
 - *Status* - sets the state for the card to enabled, disabled or lost
4. Click **Save** to confirm the operation.

The added card can now be assigned to any person belonging to the same company, department or division.

3.3.5 Assigning a Card to its Owner

1. In the *Persons* navigation tree, select the person to whom you wish to assign a credential.

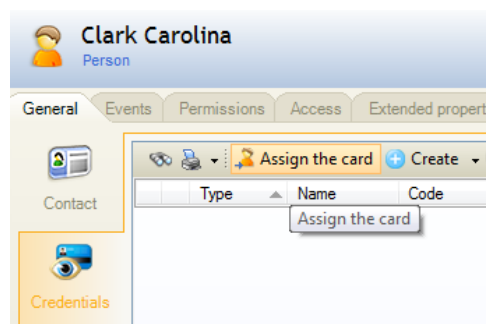


Figure 3-32 Assigning a card to the holder

2. Click the **Assign card** button to open the window in which you can search for a card to assign to the person from among all cards managed by the company, department or division. Click the card to

assign and click **OK**.

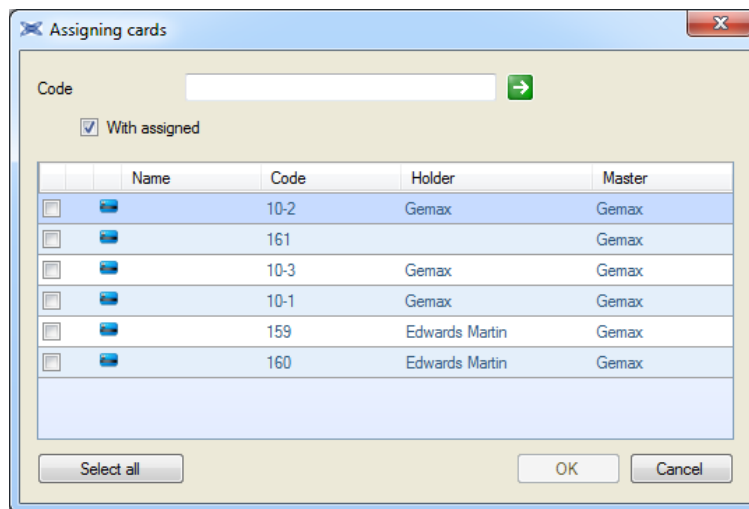


Figure 3-33 Searching for a card to assign to a person

The person becomes the card owner when he/she is assigned the card.

When the person now uses the card, it identifies this person and applies the proper access rights for the device. You can define devices (e.g., entrance door), through which the person is allowed access on the basis of the assigned credential (card), in the Access tab ([see chapter Personal Settings](#)).

Information about the last change of the credential or card can be found in the bottom of the application window as the system information (date and time of the change and the user who performed it).

3.3.6 Learning new cards directly from a device

To speed up the process of learning new cards to the ATS8600 Integrated Security Management System, it is possible to learn cards directly from a specific device - card reader. It is possible to add many cards into the system quickly by simply badging the cards on a reader. For this feature, a user of ATS8600 has to be setup with a specific reader for this and the device needs to send an event for unknown or new cards.

The procedure is as follows:

1. Select a user from which you want to learn cards.
2. Set the *Reader* in the *Personal Settings* tab of the logged-in user.

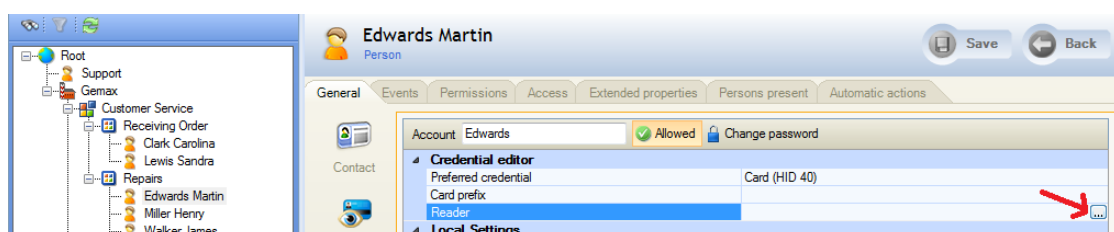


Figure 3-34 Setting the reader

3. A window with a *Devices* tree will open, and here you can select the door on whose reader the cards

will be used to learn cards.

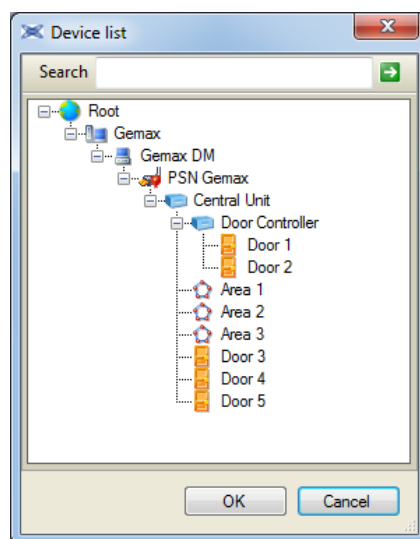


Figure 3-35 Selecting the device

4. In the *Credentials* tab, click the **Create** button to select the card type you will be learning.

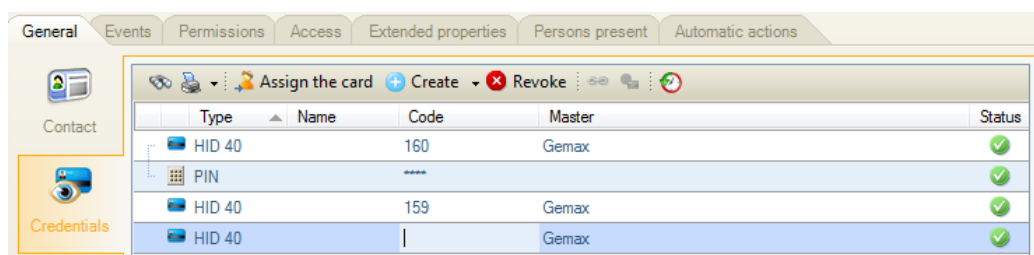


Figure 3-36 Selecting the card type

5. Activate the **Load card** function. This function remains active. This means that when you learn multiple cards, there is no need to activate the function for every card individually.

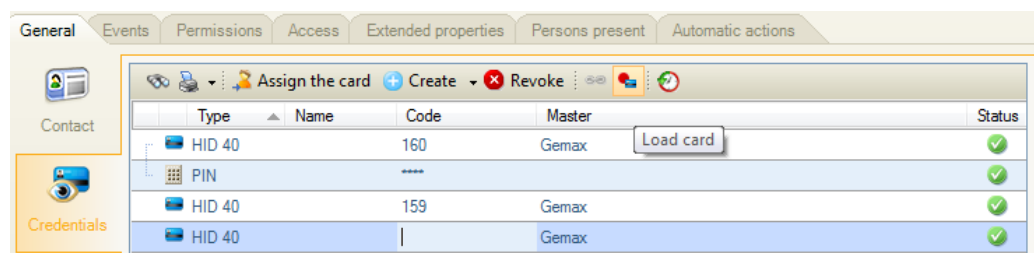


Figure 3-37 Turning card learning on

6. Badge the card on the reader. The card details will be sent to the system and the card code will be entered automatically. The next line with the card type in the credentials list will be created as well, indicating that the system is ready for the next card to be learned.

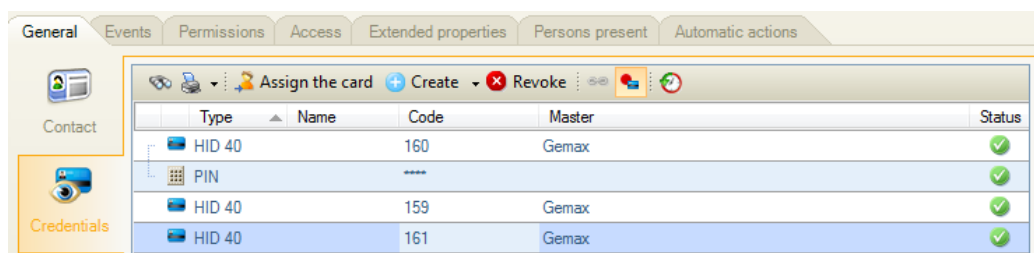


Figure 3-38 Learned card

7. After learning all cards, you can remove the last created row by clicking the **Revoke** button.

Warning:

This procedure only allows new cards to be learned, i.e., not those that already exist in the system.

Warning:

The card learn functionality is supported only if the respective device sends the card details in an event to the ATS8600 Integrated Security Management System.

3.3.7 Creating a non-transferrable credential

To assign other types of credentials to persons, select an employee in the *Persons* tree, click **Create** and select the credential from the menu.

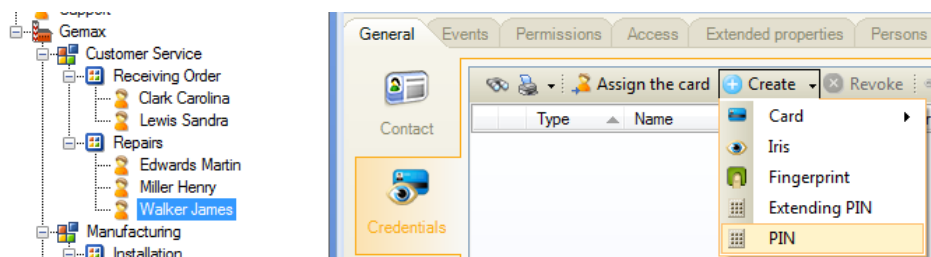


Figure 3-39 Adding a credential to a person

Similarly, as with assigning cards, it is also necessary to enter the code.

3.3.8 Merging credentials

If there is a need for merged credentials (e.g. card and PIN) it is necessary to know which PIN code belongs to which card.

The ATS8600 Integrated Security Management System makes it possible to merge such credentials that belong together. One example would be merging a card, which is a transferrable credential, with a PIN code, which is a non-transferrable credential. In such a case the card would also become a non-transferrable credential.

Using multiselect (Ctrl+click), select the credentials that you want to merge together. Click the **Merge** button.

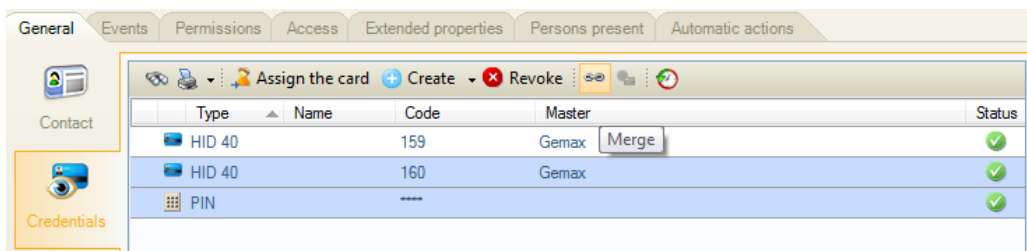


Figure 3-40 Selecting related credentials

Merged credentials will also be indicated graphically. They are displayed in blue color, one below the other.

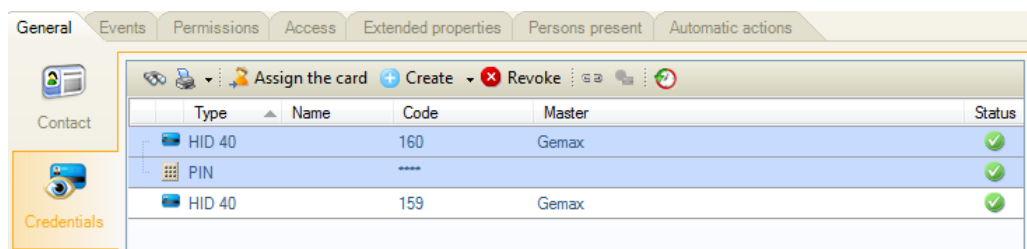


Figure 3-41 Merged credentials

Since the card with an assigned PIN becomes a non-transferable credential, it is not possible to assign it to another person. This flag that the card is non-transferable is also displayed in the company's card list.

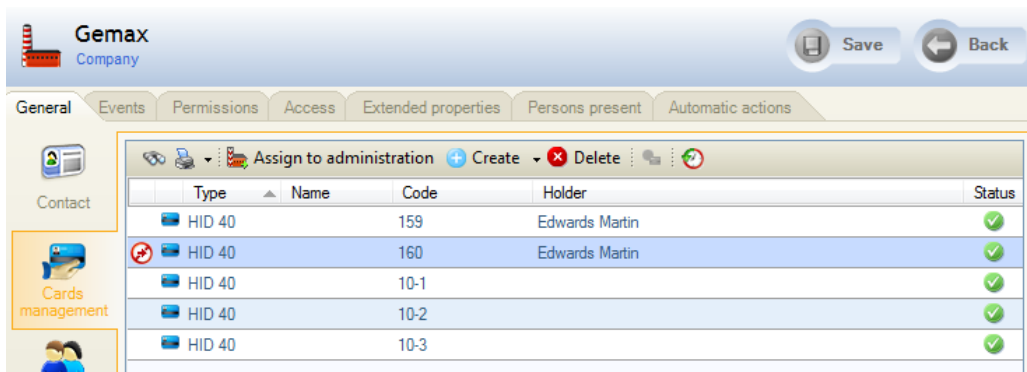


Figure 3-42 Selecting a non-transferable credential

To cancel such a link between credentials, use *Unmerge*.

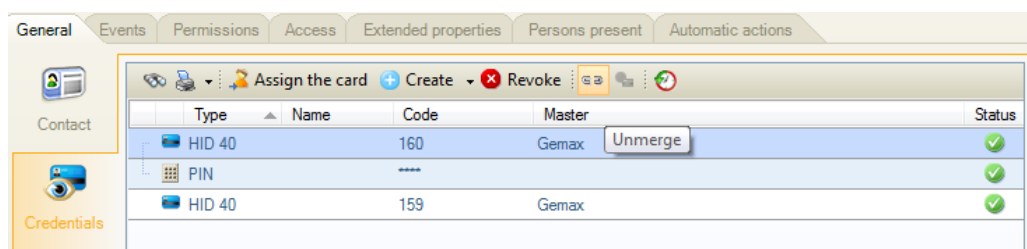


Figure 3-43 Unmerging credentials

3.3.9 Credential Status

Each credential needs to be assigned the proper status that it should acquire with respect to the usage by the person.

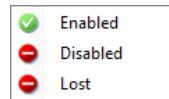


Figure 3-44 Selecting the credential status

- *Enabled* - set this status when assigning the credential to the person that needs immediate entry. After being send to the device the credential is activated and can be used to gain access on devices for which access is setup. Any use is stored together with the information about the time/date and the type of device for which the credential has been used ([see chapter Device related events](#)).
- *Disabled* - select this status to cancel (disable) the possibility to access for the selected person. The credential with this status will not allow the person to access using the device. If the person with the disabled credential attempts to use this credential when entering the object, the system will record this event into the list of events ([see chapter Device related events](#)).
- *Lost* - set this status when the credential owner reports the loss of the credential. When attempting to use the credential with Lost status, the system does not allow the person to enter the object, and this activity will be recorded in the report together with the information about the time/date and the type of device for which the lost credential was used ([see chapter Device related events](#)).

3.3.10 Credential activation

The person with assigned identifier holds the tool for usage of devices to which he/she has permission. Automatic system send to device is performed once a day at midnight (or at another time according to the settings of the device). It means that the credential can be successfully used only after being send to the device - i.e., the next day.

If you want to enable the person to enter instantly, it is necessary to perform the following operation.

1. Click the *Devices* tree tab.
2. Right-click and select the device in the tree that you want to enable to the person and select **Send credentials**.

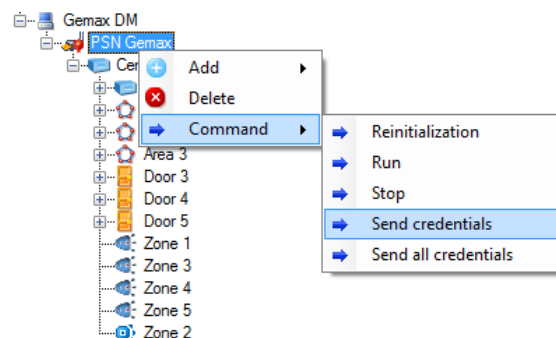


Figure 3-45 Sending credentials

When performing the operation on devices in this tree, all cards for all persons that have a changed status (active to disabled or vice versa) are send.

If this step is not performed, credentials become active or disabled automatically at midnight in the same way.

The record on this operation is displayed in the *Events* tab ([see chapter Device related events](#)) as an event log describing the beginning and the completion of sending the credentials. This record is added in the *Persons* tree in the *Events* tab in the form of a report on the **Send credentials** command.

3.3.11 Credential removal

Removal of the credential means deleting the access rights necessary for the person's entry. In case the card is removed from the person, it becomes available for future use in the company and can be assigned as a credential to another person.

To revoke a credential from the person, select the credential in the list of assigned credentials and click **Revoke**.

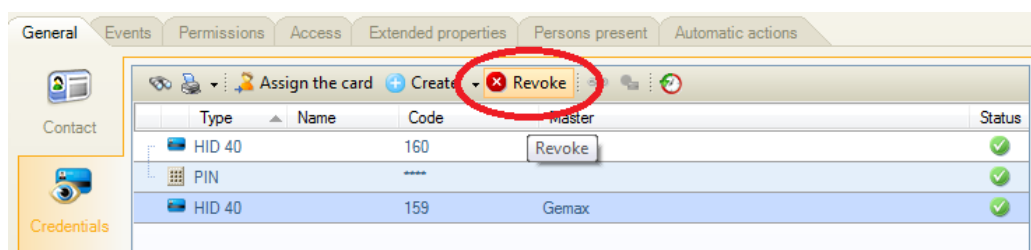


Figure 3-46 Revoking a credential

This credential remains in the system, and when assigning credentials to another persons (e.g., new employees) it is automatically displayed in the list of credentials. In this case, it is sufficient to check the box again and the credential will be assigned to the new person.

3.3.12 Deleting a card

To delete a card, click it in the *Card Management* list of the respective organisational unit and select the **Delete** menu command. When this function is selected, the card will disappear from the list of available cards.

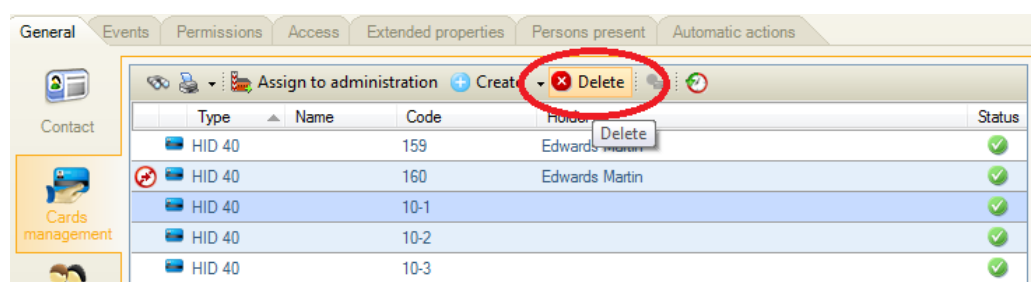


Figure 3-47 Deleting a card

When person with an assigned cards are deleted, this card subsequently becomes available and appears in the list of cards of the respective cards manager.

In case the complete company is deleted, all cards are moved under the main tree node - *Root*.

3.4 Role assignment

The infotype tab, *Roles*, allows to define a standard role according to a person's access rights to the ATS8600 System. The role is a set of permissions that are assigned to persons or groups of persons. Each role is defined by access rights for application functions.

To assign a role to the user, click the person in the tree, select the *Roles* infotype on the right side of the screen and check the box of the selected role category to select the role of the user in the system:

- HR Manager
- Company Manager
- Reception
- Administrator
- Service Technician
- Access Manager
- Dispatcher

Each person can be assigned more than one role. Permissions available in any assigned role will be available for this person.

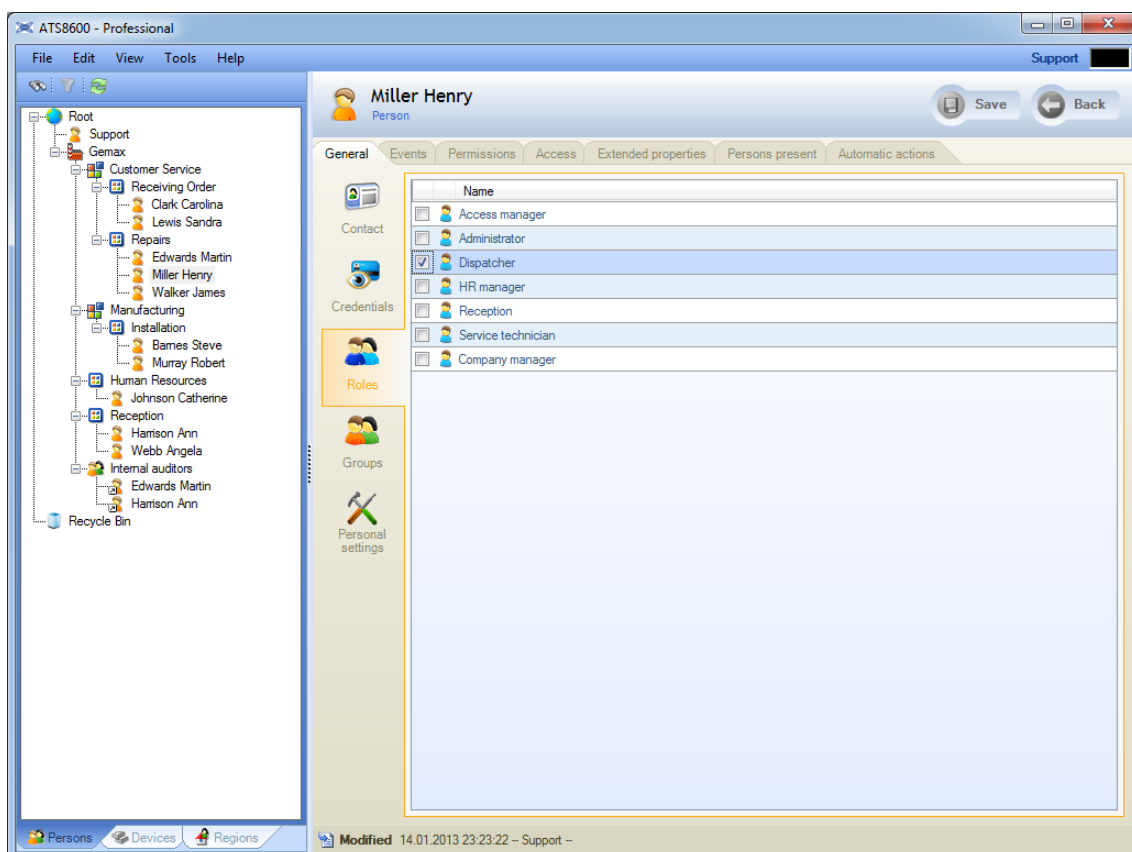


Figure 3-48 Assigning a role to the user

3.4.1 Descriptions of Roles

In the ATS8600 Integrated Security Management System, individual users can be assigned the following roles:

1. Administrator

- Has the highest permissions within the application
- Can perform all operations
- Has the right to view the whole history
- Has no permission to configure region count

2. Dispatcher

- Has the right to monitor the status of devices (*Monitor*, Real-Time monitor)
- Has the right to monitor the history of events concerning the devices
- Can operate the devices

3. HR Manager

- Has the right to edit data in the *Persons*
- Has the right to add persons
- Can view the history of changes concerning the persons and devices
- Modify personal settings
- Personal Settings
- Modify person details
- View person details
- View picture
- Manage groups
- Events

4. Reception

- Has the right to view persons' information
- Can detect the presence of persons in regions
- Create visits
- Visitors management

5. Service Technician

- Device Management
- Device settings
- Events
- Edits in the Visualization and Patrol tours panel
- Edits in the tree Regions

6. Access Manager Has the following permissions:

- Extended properties on devices
- Manage time restrictions
- Manage access rights
- Modify personal settings
- Personal Settings
- Visitors management
- Reception management
- Modify person details
- View person details
- View picture
- Manage groups

- Credentials
- Modify credentials
- Device Management
- Events
- Has no permission set up to count entrances

7. Company Manager

- Has permission to administrate the company of which he/she is the manager (to which he/she is assigned in ATS8600)
- Manage extended properties
- Manage time restrictions
- Manage access rights
- Modify personal settings
- Personal Settings
- Modify person details
- View person details
- View picture
- Manage groups
- Credentials
- Modify credentials
- Device Management
- Events
- Has no permission set up to count entrances

Note:

After assigning the Company Manager role, it is necessary to press **Refresh** in order for the system to update the set permissions and display them correctly.

Detailed schedule of permissions for individual roles according to the subject of the permission is listed in table below.

	Roles						
	1.	2.	3.	4.	5.	6.	7.
Application							
Tools	✓						
Manage automatic actions	✓						
Reception management	✓						
Modify personal settings	✓						
View personal settings	✓						

Modify system settings	✓						
View system settings	✓						
Visits	✓						
Visitors management	✓					✓	
Reception management	✓					✓	
Create visits	✓			✓			
View list of current visitors	✓			✓			
Persons management	✓						
Modify credentials	✓					✓	
View credentials	✓					✓	
Modify person details	✓		✓			✓	
View person details	✓		✓			✓	
View picture	✓		✓			✓	
Manage roles	✓						
View roles	✓						
Manage groups	✓		✓			✓	
Security	✓						
Manage application permissions	✓						
Manage time restrictions	✓					✓	
Manage extended properties	✓					✓	
Manage access rights	✓					✓	
Manage permissions	✓						
Diagnostics	✓						
Image Monitor	✓						
Licenses	✓						
Activate license	✓						
Device management	✓						
Manage device tree	✓				✓	✓	
Modify device settings	✓				✓		
Visualization	✓						
Monitor	✓	✓					
Manage patrol tours	✓	✓					
Alarm management	✓	✓					

Resolve alarms	✓	✓					
Events	✓	✓	✓			✓	
Real-Time monitor	✓	✓					
Modify visualization	✓				✓		
Modify patrol tours	✓				✓		
Activate alarm sound	✓						✓
Event history	✓		✓		✓	✓	
Modify regions	✓				✓		✓
Manage regions	✓				✓	✓	
Manage facility panel	✓				✓		
Cash Desk Monitor	✓						
Display events without permission check	✗	✗	✗	✗	✗	✗	✗
View PIN codes	✗	✗	✗	✗	✗	✗	✗
Automatic report printing	✗	✗	✗	✗	✗	✗	✗
Time restrictions							
Create	✓					✓	✓
Read	✓					✓	✓
Edit	✓					✓	✓
Permissions	✓					✓	✓
Delete	✓					✓	✓
Event filters							
Create	✓						
Read	✓	✓	✓	✓	✓	✓	✓
Edit	✓						
Permissions	✓						
Delete	✓						
Credentials							
Create	✓					✓	✓
Read	✓			✓		✓	✓
Edit	✓			✓		✓	✓
Permissions	✓					✓	✓
Assign	✓			✓		✓	✓

Delete	✓					✓	✓
Visitors							
Create	✓			✓		✓	
Read	✓	✓		✓		✓	
Edit	✓			✓		✓	
Delete	✓					✓	
Patrol tours							
Create	✓				✓		
Read	✓	✓			✓		
Edit	✓				✓		
Permissions	✓				✓		
Delete	✓				✓		
Commands	✓						
Monitor	✓				✓		
Persons							
Create	✓		✓			✓	
Read	✓	✓	✓	✓		✓	
Edit	✓		✓			✓	
Delete	✓		✓			✓	
Permissions	✓					✓	
Define Access	✓					✓	
Commands							
Read	✓	✓			✓	✓	
Permissions	✓						
Receptions							
Create	✓			✓		✓	
Read	✓	✓		✓		✓	
Edit	✓			✓		✓	
Delete	✓					✓	
Permissions	✓					✓	
Define Access	✓			✓		✓	
Regions							
Create	✓				✓		

Read	✓	✓			✓	✓	
Edit	✓				✓		
Permissions	✓				✓		
Delete	✓				✓		
Define Access	✓					✓	
Replications							
Create	✓						
Read	✓						
Edit	✓						
Permissions	✓						
Delete	✓						
Commands	✓						
Monitor	✓						
Events							
Read	✓	✓	S		✓	✓	
Permissions	✓						
Devices							
Create	✓				✓		
Read	✓	✓			✓	✓	
Edit	✓				✓		
Permissions	✓				✓		
Define Access	✓				✓		
Delete	✓				✓		
Commands	✓	✓					
Monitor	✓	✓					
Count Attendance	✗	✗	✗	✗	✗	✗	✗

Table 3-1 Predefined permissions list from the point of view of individual roles

Note:

S - this role is enabled to see only selected event types in the system

Tip:

If it is necessary to create more predefined permission groups for ATS8600, we recommend setting them up in groups, to which the respective ATS8600 users will be assigned.

Warning:

Enabling the *Display events without permission check* permission disables the filter that normally filters events by permissions to persons, devices, regions, identifiers, event types. This permission enables the user to see all the events concerning the respective item.

3.5 Personal Settings

The *Personal Settings* tab holds individually set user parameters for working with the application.

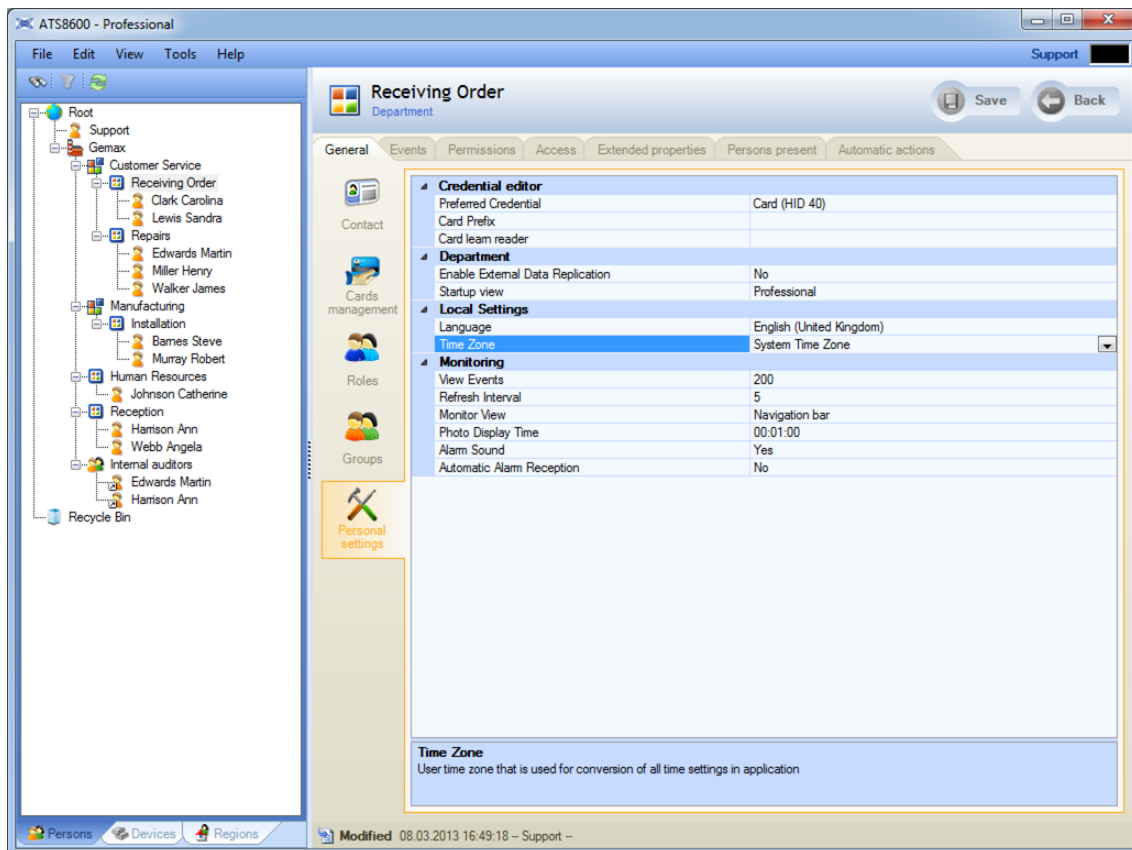


Figure 3-49 Personal Settings

Personal user settings are also available from the menu *Tools - Settings - Personal Settings* tab.

3.5.1 Setting access to the Application

The upper part of the screen, above the list of personal Settings, includes a window for entering the account or changing the password. Fields in this window indicate whether a specific person is also an application user.

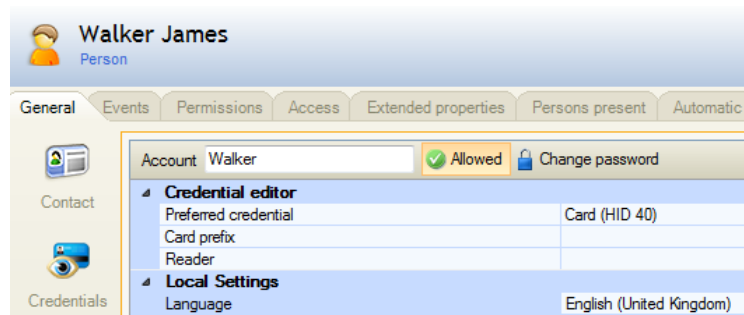


Figure 3-50 Entering an account

Functions:

Account - user's account name used to log in to the application (username)

Allowed - this field indicates whether the user is allowed to access the application. To deny access to the user, change the field to Denied.

Change password - click this field to open the window to change a person's password. The entered user password must be secure and must include:

- At least 7 characters
- At least one uppercase letter
- At least one lowercase letter
- At least one numeric character (number)
- At least one special character (! @ # \$ % ^ & * _)
- Cannot be the same as the account name

If the password entered fails to meet the above requirements, a red icon appears in the the password entry dialogue box.

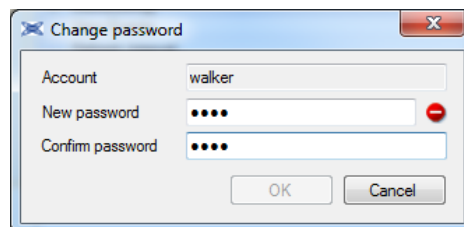


Figure 3-51 Insufficiently secure password

As soon as the entered password meets the security criteria, the icon turns green, which indicates that the password is appropriate from a security perspective.

Retype the password into *Confirm password*. If the password matches the password in New password box and is secure enough, the **OK** button becomes active. Clicking **OK** to confirm the password change.

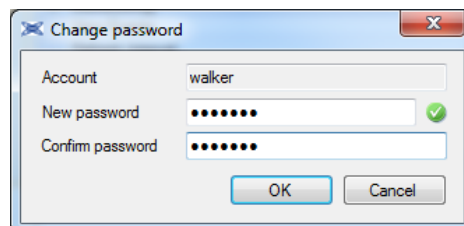


Figure 3-52 Secure password

3.5.2 Administration of personal settings

Personal settings of an OS element are by default inherited from its parent OS element. These are referred to as inherited values.

To change the preset settings, click the setting that you want to change to activate the edit mode. Overwrite the value that you want to change.

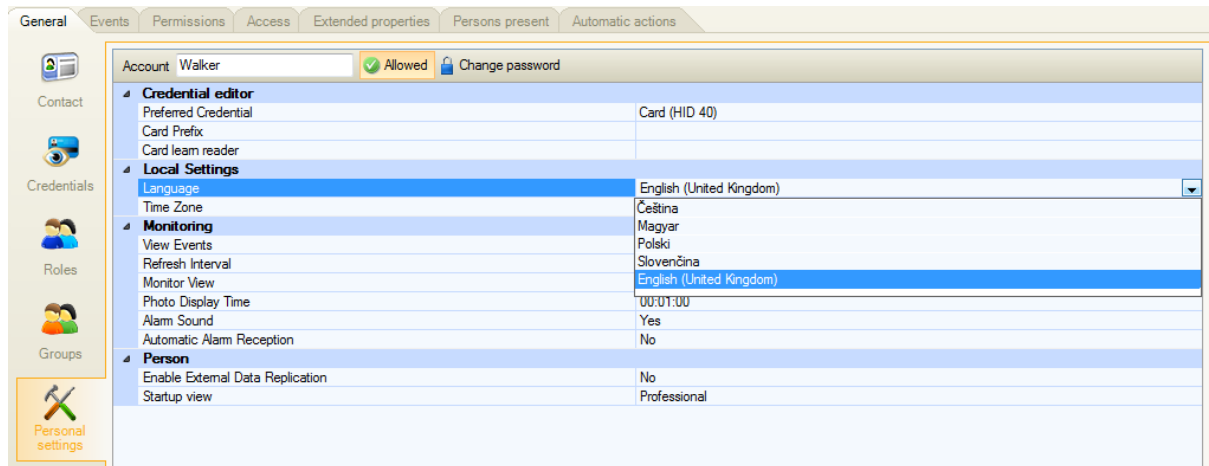


Figure 3-53 Changing settings

The changed setting will appear in bold so that it is apparent which settings have been changed from default settings. All levels below the node, where the change took place, will inherit this setting.

Example:

If the language is changed from Slovak to English in the Repairs department, each person belonging to the Repairs department will inherit the English setting.

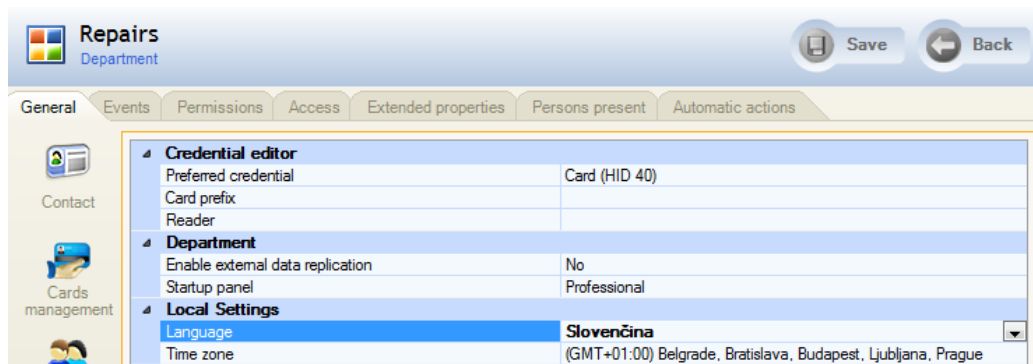


Figure 3-54 Changing personal settings

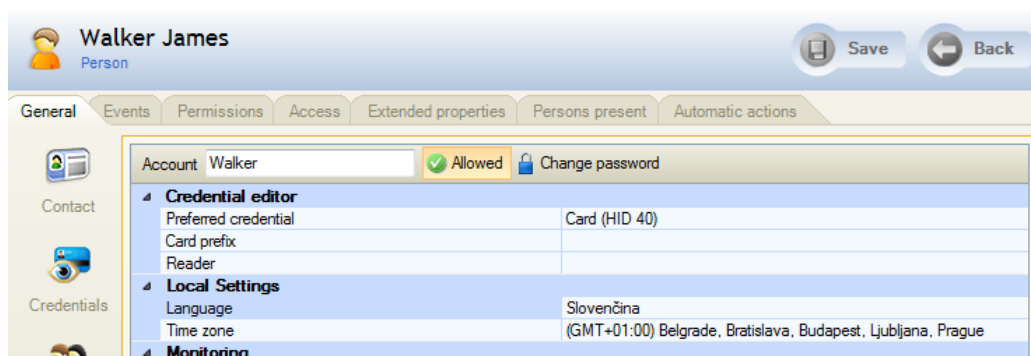


Figure 3-55 Inherited settings

If you decide that you want to restore the default language in the Repairs department, right-click on *Inherit*. Language is restored to the default value inherited from the parent OS in the *Persons tree*.

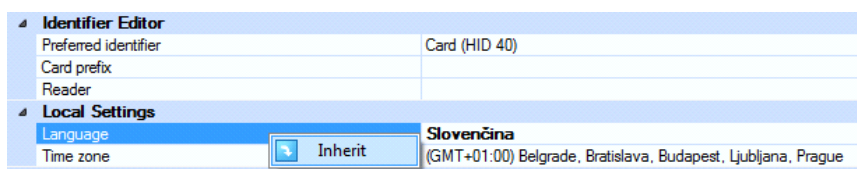


Figure 3-56 Selecting inherited settings

Settings

- *Preferred credential* - sets the default type of credential that the user is going to use. By setting this item, the system will automatically select the this as default value.
- *Time zone* - For each user, the time zone, in which they work and which is used as a reference for displaying the time, has to be set. This is because the data is recorded in UTC and all time records concerning events are automatically recalculated to UTC.
- *Enable replication* - allows data synchronization between ATS8600 system with another information system.
- *Startup panel* - defines which panel is displayed on log in to the application. The option menu depends on the application version.
- *Refresh period* - time in seconds between two refreshes of the event list
- *View events* - number of displayed rows in the *Events*
- *Alarm tone* - enable or disable audible alerting of alarms.

The chosen personal settings need to be saved by clicking **Save**.

Note:

Explanation of individual settings is displayed in the lower right corner of the application after clicking each setting.

3.6 Permissions management

Permissions are an independent tab of the Professional panel. The *Permissions* tab is the central location for assigning permissions to single objects. By setting permissions, single users gain access rights to functions within the ATS8600 Integrated Security Management System based on their task. Permissions can be set with great detail, so it is necessary to pay special and adequate attention to

this function. The easiest method for defining permissions is to select this for groups of people like departments as new users under these groups will automatically inherit the parent permissions.

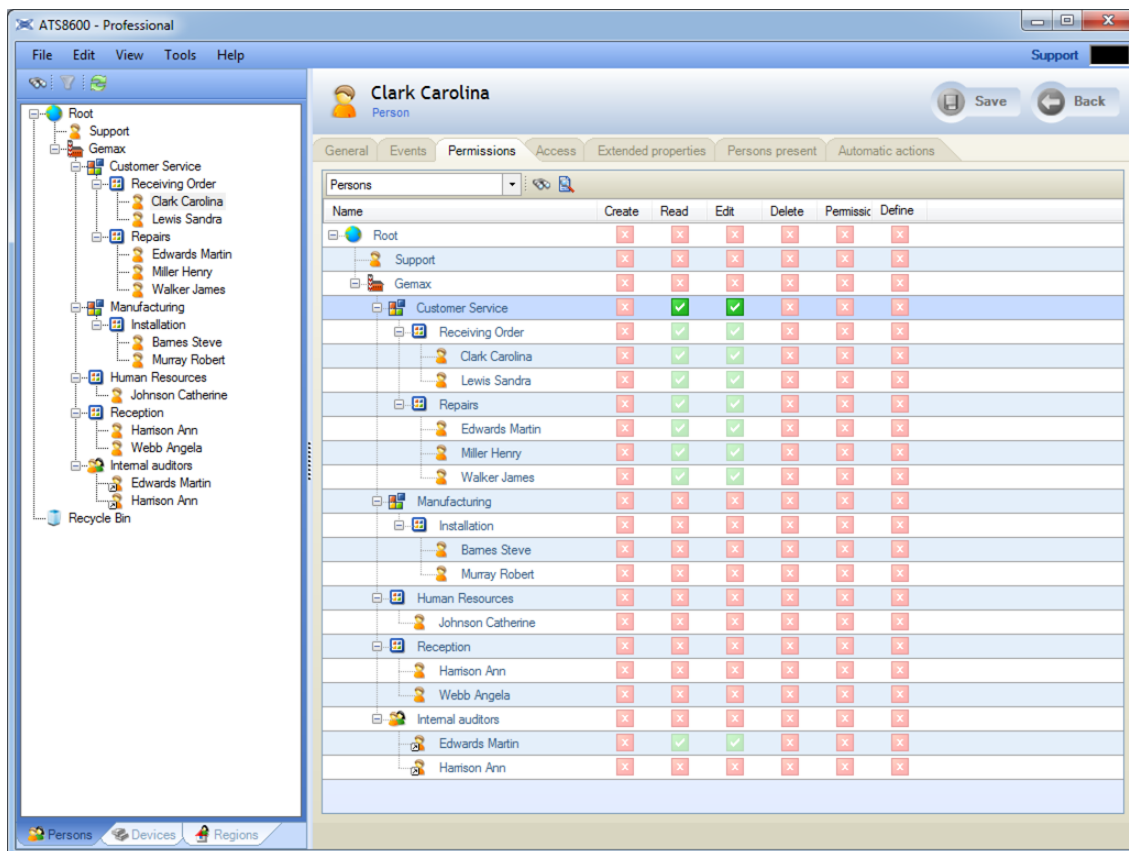


Figure 3-57 Permissions

3.6.1 Permissions group settings

It is possible to set permissions for any organizational structure item (company, department, person). Permissions are grouped based on functionality such as:

- **Application** - *Application* permissions define access rights to individual tabs (navigation panel tabs and infotypes tabs) in the ATS8600 application. Setting application permissions for a certain person defines the final appearance of the right-hand part of the application window. Permission setting in particular define which tabs will be visible and accessible to the user. These settings therefore are used to administer the access to modules and available functionality within screens.
- **Persons** - When setting permissions for persons, the selected user is granted access rights to the *Persons* tree. With respect to the granted application permissions, the user can view or change information of persons in the tree.
- **Events** - It is possible to set user permissions with regards to events.
- **Devices** - By setting permissions to devices, a particular user is granted access rights to the *Devices* tree. With respect to the granted application permissions, a user can view or change information of devices in the tree.
- **Commands** - By setting permissions to *Commands* you can allow individual persons to view or issue commands via the application. Permissions can be set individually for each command.
- **Replications** - permissions related to the administration of the *Replications* module.

- *Regions* - by setting permissions for regions, a particular user is granted access rights to the *Regions* tree. Based on the given permissions, the devices in the *Regions* tree can be viewed or managed.
- *Event filters* - specific users can have their permissions set for individual event filters.
- *Credentials* - specific users can have their permissions set for individual credentials.
- *Patrol tours* - setting patrol tours permissions to a specific user grants the user permissions to manage patrol tours.
- *Time restrictions* - specific users can receive permissions for time restrictions.
- *Visitors* - specific users can have their permissions set for visitors.
- *Receptions* - specific users can have their permissions set for receptions.

Select the permission group from the drop-down menu in the *Permissions* tab.

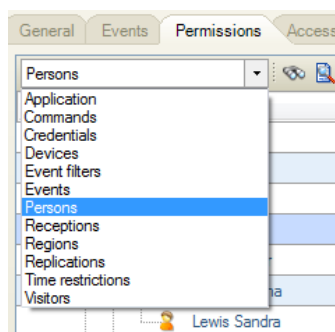


Figure 3-58 Selecting a permission group

3.6.2 Types of permission

When a permission group is selected, OS items (company, department, person) can be granted the following types of permissions:

1. Permissions for *Application*

- Status
 - defines ATS8600 functionality which the user will be allowed to use.

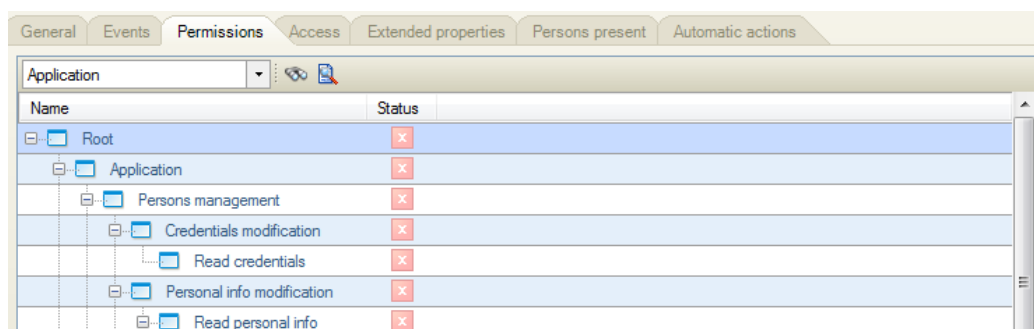


Figure 3-59 Types of permission for the application

2. Permissions for *Persons*

- Create
 - permission to create a new person.
- Read

- permission to view allowed information concerning persons shown in the *Persons* tree.
- Edit
 - permission to edit allowed information concerning persons shown in the *Persons* tree. For editing it is also necessary to grant read permission.
- Delete
 - permission to delete a person.
- Permissions
 - permission to set permissions for persons.
- Define Access
 - permission to set access rights for persons.

Name	Permissic	Define	Create	Read	Edit	Delete
Root	☐	☐	☐	☐	☐	☐
Support	☐	☐	☐	☐	☐	☐
Gemax	☐	☐	☐	☐	☐	☐
Customer Service	☐	☒	☒	☐	☐	☐
Receiving Order	☐	☒	☒	☐	☐	☐
Clark Carolina	☐	☒	☒	☐	☐	☐
Lewis Sandra	☐	☒	☒	☐	☐	☐

Figure 3-60 Type of permissions for Persons

3. Permissions for *Events*

- Read
 - permission to view events concerning allowed persons or devices.
- Permissions
 - define whether a person can assign a specific permission to other persons.

Name	Read	Permissic
Root	☐	☐
Access events	☐	☐
Access allowed to [%PERSON%]	☐	☐
[%PERSON%] entered [%REG...]	☐	☐
[%PERSON%] left [%REGION...]	☐	☐
Access granted for unknown cr...	☐	☐

Figure 3-61 Types of permission for Events

4. Permissions for *Devices*

- Create
 - permission to add new devices.
- Read
 - permission to view information concerning the chosen device.
- Edit
 - permission to edit device settings (edit data, change permissions).
- Delete
 - permission to delete a device from the tree.

- Permissions
 - permission to define device permissions.
- Define Access
 - permission to define the access to devices.
- Commands
 - permission to send commands to devices. For example, Select a door and send the door open command.
- Monitor
 - permission for the user to monitor (view) the device status.
- Count Attendance
 - availability of Count entrances function.

An object is chosen from the menu of the Permission groups field.

Name	Create	Read	Edit	Delete	Permissic	Define	Comman	Monitor	Count
Root	x	x	x	x	x	x	x	x	x
Gemax	x	x	x	x	x	x	x	x	x
Gemax DM	x	x	x	x	x	x	x	x	x
PSN Gemax	x	✓	✓	x	x	x	✓	✓	x
Central Unit	x	✓	✓	x	x	x	✓	✓	x
Door Controller	x	✓	✓	x	x	x	✓	✓	x
Door 1	x	✓	✓	x	x	x	✓	✓	x
Reader	x	✓	✓	x	x	x	✓	✓	x

Figure 3-62 Types of permission for Devices

5. Permissions for *Commands*

- Read
 - permission to view and send commands
- Permissions
 - enables a person to assign the given permission to other persons.

Name	Read	Permissic
Push	x	x
Switch to Day Mode	x	x
Switch to Night Mode	x	x
Refresh	x	x
Connection parameters authenti...	x	x
Reinitialization	x	x
Remove person from region	x	x

Figure 3-63 Types of permission for Commands

6. Permissions for *Replications*

- Create
 - permission to create new information system replications.
- Read
 - permission to view item data from the Replications tree.

- Edit
 - permission to change items from the Replications tree.
- Permissions
 - permission to assign these permissions for other users.
- Delete
 - permission to delete an information system replication entry from the tree.
- Commands
 - permission to send commands to the tree items, such as Confirm Replication.
- Monitor
 - permission to view statuses of the replication tasks (e.g., "Replicating", "No activity," or "Waiting for confirmation").

Name	Create	Read	Edit	Permissic	Delete	Comman	Monitor
Root	x	x	x	x	x	x	x

Figure 3-64 Types of permission for Replications

7. Permissions for *Regions*

- Create
 - permission to create new regions.
- Read
 - permission to view data concerning the Regions tree.
- Edit
 - permissions to edit items from the Regions tree.
- Delete
 - permission to delete objects from the Regions tree.
- Permissions
 - permission to assign these permissions for other users.
- Define Access
 - permission to assign access rights to regions for other users.

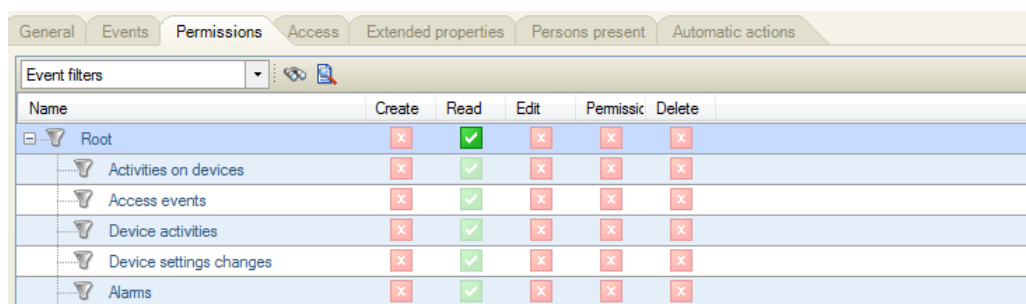
Name	Create	Read	Edit	Delete	Permissic	Define
Gemax	x	x	x	x	x	x
Prague	x	x	x	x	x	x
1st floor	x	x	x	x	x	x
Office 101	x	x	x	x	x	x
Door 3	x	✓	✓	x	x	x
Door 1	x	✓	✓	x	x	x

Figure 3-65 Types of permission for Regions

8. Permissions for *Event filters*

- Create
 - permission to create new event filters.
- Read
 - permission to view existing event filters.

- Edit
 - permission to edit event filters.
- Permissions
 - permission to assign the event filter permission to other users.
- Delete
 - permission to delete an event filter from the list.



Name	Create	Read	Edit	Permissions	Delete
Root	X	✓	X	X	X
Activities on devices	X	✓	X	X	X
Access events	X	✓	X	X	X
Device activities	X	✓	X	X	X
Device settings changes	X	✓	X	X	X
Alarms	X	✓	X	X	X

Figure 3-66 Types of permission for Event filters

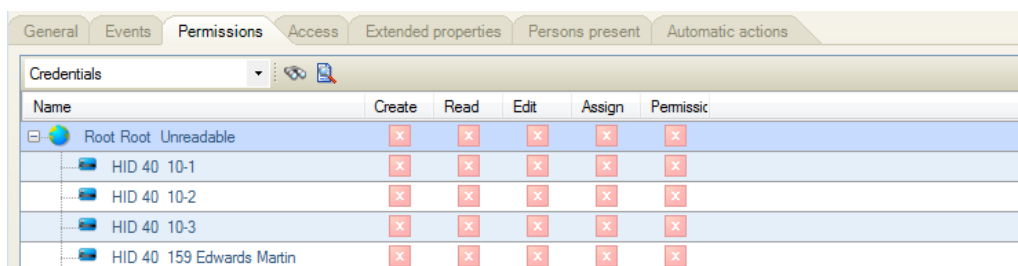
Warning:

You are unable to set permissions for the following predefined filters:

- All activities (in *Persons*, *Devices* and *Regions* trees)
- Card activities (in *Persons* tree in *Credentials* tab)
- Automatic actions activities (in *Automatic actions* tab, *History* window)

9. Permissions for *Credentials*

- Create
 - permission to create new credentials.
- Read
 - permission to view existing credentials.
- Edit
 - permission to edit existing credentials.
- Permissions
 - permission to assign credential permissions to other users.
- Delete
 - permission to delete credentials.



Name	Create	Read	Edit	Assign	Permissions
Root Root Unreadable	X	X	X	X	X
HID 40 10-1	X	X	X	X	X
HID 40 10-2	X	X	X	X	X
HID 40 10-3	X	X	X	X	X
HID 40 159 Edwards Martin	X	X	X	X	X

Figure 3-67 Types of permission for Credentials

10. Permissions for *Patrol tours*

- Create
 - permission to create new patrol tours.

- Read
 - permission to view a patrol list.
- Edit
 - permission to edit patrol properties.
- Permissions
 - permission to assign patrol permissions to other users.
- Delete
 - permission to delete patrol tour from the patrol list.
- Commands
 - permission to send commands for patrol tours.
- Monitor
 - permission for a user to view the status of started patrol tours.

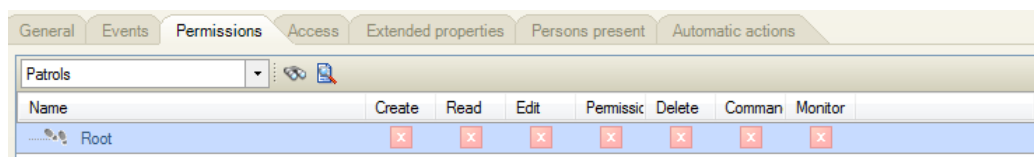


Figure 3-68 Types of permission for Patrol tours

11. Permissions for Time restrictions

- Create
 - permission to create new time restrictions
- Read
 - permission to view existing time restrictions.
- Edit
 - permission to edit time restrictions.
- Permissions
 - permission to assign permissions for time restrictions to other users.
- Delete
 - permission to delete a time restriction from the list.

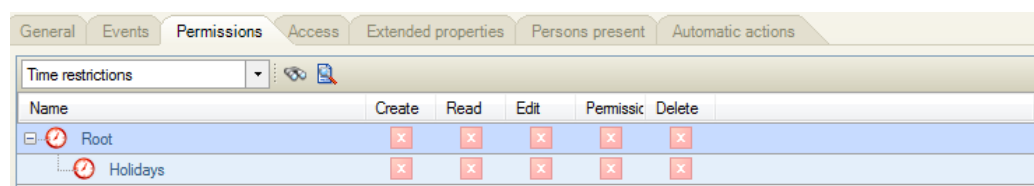
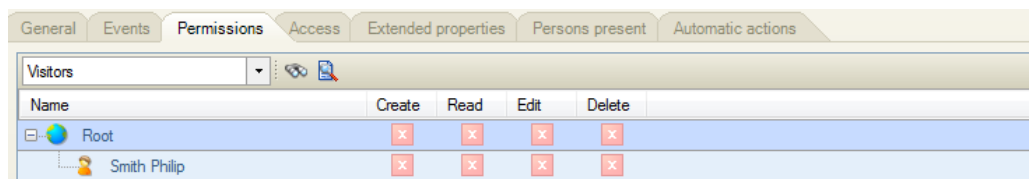


Figure 3-69 Types of permission for Time restrictions

12. Permissions for Visitors

- Create
 - permission to create new visitors.
- Read
 - permission to view existing visitors.
- Edit
 - permission to edit existing visitors.
- Permissions
 - permission to assign visitors' permissions to other users.

- Delete
 - permission to delete a visitor from the visitors tree.

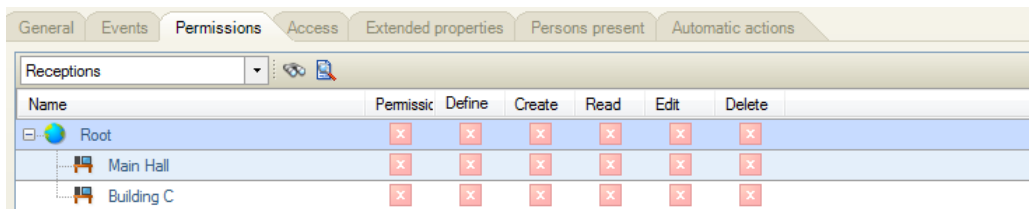


Name	Create	Read	Edit	Delete
Root	x	x	x	x
Smith Philip	x	x	x	x

Figure 3-70 Types of permission for Visitors

13. Permissions for *Receptions*

- Create
 - permission to create new receptions.
- Read
 - permission to view existing receptions.
- Edit
 - permission to edit existing receptions.
- Permissions
 - permission to assign reception permissions to other users.
- Delete
 - permission to delete receptions.
- Define Access
 - permission to set reception access permissions for other users.



Name	Permissic	Define	Create	Read	Edit	Delete
Root	x	x	x	x	x	x
Main Hall	x	x	x	x	x	x
Building C	x	x	x	x	x	x

Figure 3-71 Types of permission for Receptions

3.6.3 Permission state

Object permissions can have the following basic states:

- Permission allowed -  - A person has permission for the chosen object and permission type. This permission was created by a direct setting, which is indicated by a dark green icon.
- Time-restricted allowed permission (available only on the *Access* tab) -  - A person has temporary restricted permission for the chosen "Persons" object and the chosen "Access permission" permission type. This permission was created by a direct setting, which is indicated by a dark green icon. When the upper right corner is red, the permitted access is temporary.
- Allowed permission without inheritance (available only on the *Permissions* tab) -  - A person has permission for the chosen object and permission type. This permission is only related to the object on which it is set and is not transferred to its child elements. This permission was created by a direct setting, which is indicated by a dark green icon.
- Permission allowed by inheritance -  - A person has permission for the chosen object and

permission type. This permission was created by inheriting the permission from a parent, which is indicated by a pale green icon.

- Time-restricted inherited allowed permission (available only on the *Access* tab) -  - A person has a temporary permission for the chosen "Persons" object and the chosen "Access permission" permission type. This permission was created by inheriting permission from a parent, which is indicated by a pale green icon. When the upper right corner is red, the permitted access is temporary.
- Permission denied -  - A person has no permission for the selected object and permission type. This restriction was created by a direct setting, which is indicated by a dark red icon.
- Denied permission without inheritance (available only on the *Permissions* tab) -  - A person does not have permission for the chosen object and permission type. This restriction is only related to the object on which it is set and is not transferred to its child elements. This restriction was created by a direct setting, which is indicated by a dark red icon.
- Inherited denied permission -  - A person does not have permission for the chosen object and permission type. This restriction was created by inheriting restriction from a parent, which is indicated by a pale red icon.

3.6.4 Principle of inheriting

Single objects are added into the system in a hierarchical structure (organisational structure). It is also easy to recognise the hierarchy graphically.

To simplify the granting of permissions, the system supports permission inheritance. This means that by setting permissions for a parent object these permissions are automatically inherited by child objects.

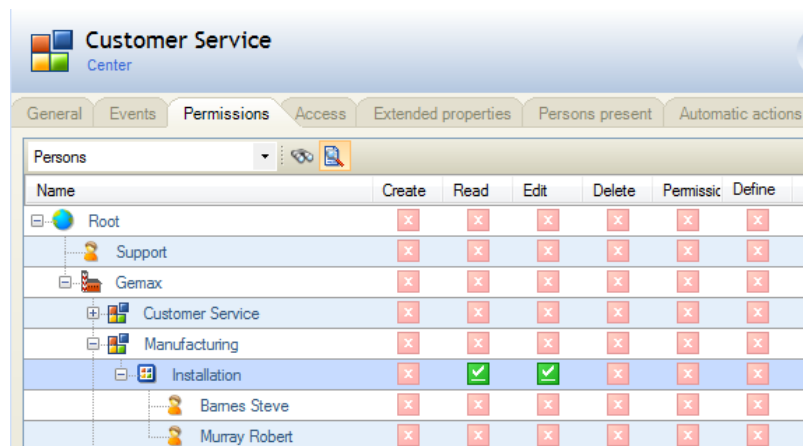
In case an inherited permission is not suitable for a particular object, it can be changed individually. A permission can be set at any node and child in the tree.

Examples of inherited permissions are shown in figure below.



Figure 3-72 Inheriting a permission

It is also possible to use the principle of parent permissions when the permission/restriction is not transferred hierarchically to the children of an object on which the permission is set.



Name	Create	Read	Edit	Delete	Permissic	Define
Root	X	X	X	X	X	X
Support	X	X	X	X	X	X
Gemax	X	X	X	X	X	X
Customer Service	X	X	X	X	X	X
Manufacturing	X	X	X	X	X	X
Installation	X	✓	✓	X	X	X
Barnes Steve	X	X	X	X	X	X
Murray Robert	X	X	X	X	X	X

Figure 3-73 Non-inheritance of a permission for children

Warning:

Only authorised users have rights to execute the above actions.

Show details - click  to view detail information on the permission and its changes when hovering the mouse over the permission.

Persons	Object	Modified	
  Barnes Steve	 Gemax	12.05.2011 13:30:55	Support
  PersonRoot	 PersonRoot	01.01.0001 00:00:00	-----

Figure 3-74 Permission detail

3.6.5 Permission setting

1. In a tree choose a person you want to set permissions for and click to select this person.
2. On the Permissions tab of the navigation panel select the permission group in the first field, i.e., the object for setting permissions.
3. The selected tree (from step 2) with the permissions options will appear.
4. Setting of the required permission:
 - Right-click the object to view the menu of permission statuses you can use for the selected object

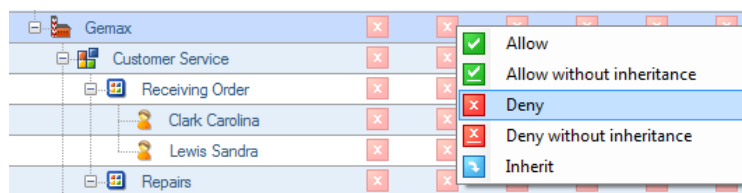


Figure 3-75 Permission status change

- The permission status can also be changed by simply clicking the permission icon (cycling between Allow, Allow without inheritance, Deny, Deny without inheritance, Inherit).

If the object for which you have performed the permission change has other hierarchically child objects, they will also inherit the permission setting ([see chapter Principle of inheriting](#)).

Note:

Final permissions are a result of inheriting and setting permissions. By changing permissions (even inherited), the highest priority has the setting at the lowest hierarchic level: Organisational structure -> Group -> Role -> Person. The highest priority has the permission setting for a person. It is superior to permission settings for the OS, group or role.

Tip:

It is recommended that the setting of permissions for a group is done only in special cases and as a temporary rather than a permanent solution to a situations. One person can belong to several groups and the setting of different permissions for various groups can cause conflicting states and situations. Most permission settings are recommended to be performed at the organisational structure level. Exceptions can be set directly for a person.

3.6.6 Example of configuring permissions

Configuring permissions is explained through the use of an example.

1. Create a new person

The application administrator will create a new person (James Walker), using their own account, in the organisational structure of a company that is named Gemax for this example.

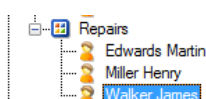


Figure 3-76 New person

The new person has been created but has no permissions yet to work in the application, not even to log in. It is necessary to create an account for the person to provide access to the ATS8600Integrated Security Management System.

2. Create an account for a new person

Click on James Walker in the *Persons* tree for whom you wish to create an account. Open the *Personal Settings* tab in the application window on the right.

Configure following fields in the dialogue box:

- *Allowed* - Check the box to enable the use of the created.
- *Account* - Enter the user name with which the person will log into the application.
- *Change password* - Enter the password for that person to log into the application (or change for an existing account).

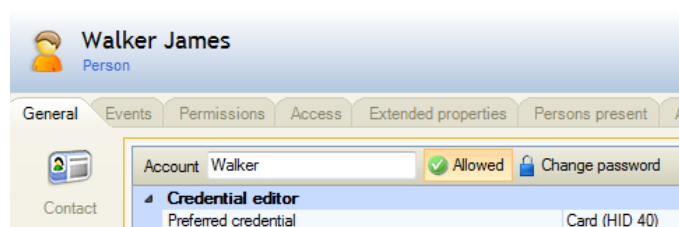


Figure 3-77 Creating an account for a new person

3. Login of a created person

James Walker for whom the account is just created is now able to log into the application using his

own login name and password.

When logging in, login was successful but an empty application window appears because a James Walker (the new person) has no valid permissions assigned.

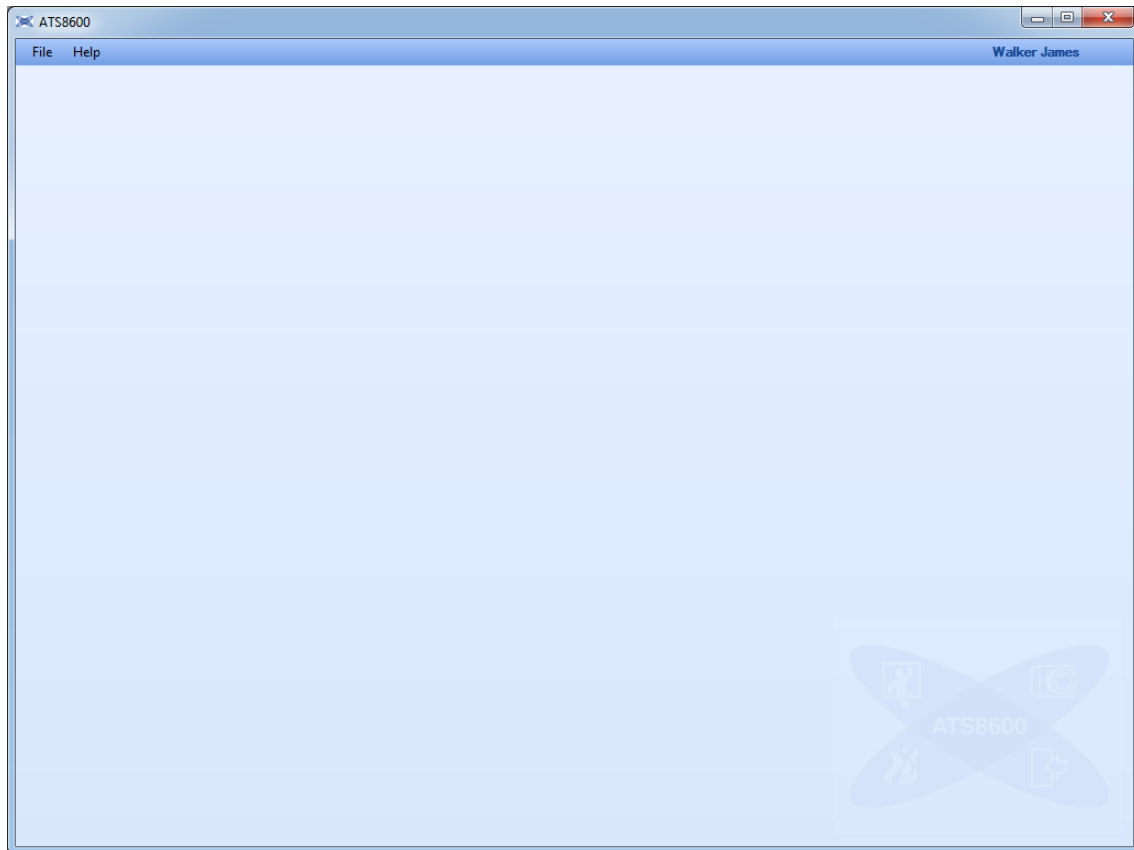


Figure 3-78 Application window of a user with no permissions

Firstly, James Walker needs to be granted permissions for the application by the administrator or another authorised person.

4. Setting a persons' permissions for *Application*.

Select James Walker in the *Persons* tree and click the *Permissions* tab. This tab displays Walker's permissions for the Application. From the red icons it is clear that Walker has no permissions for the application. Therefore, after logging in to the application, a plain screen will appear without any tabs.

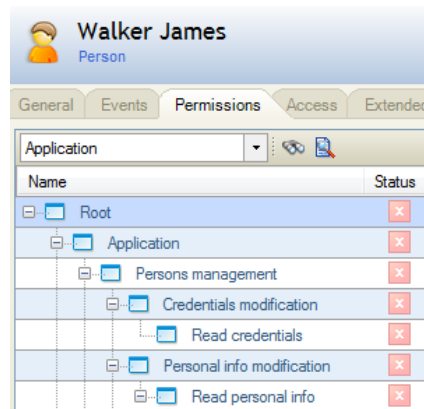


Figure 3-79 Person permissions for application

Set this person permissions for Application (e.g., for the *Contact* tab)

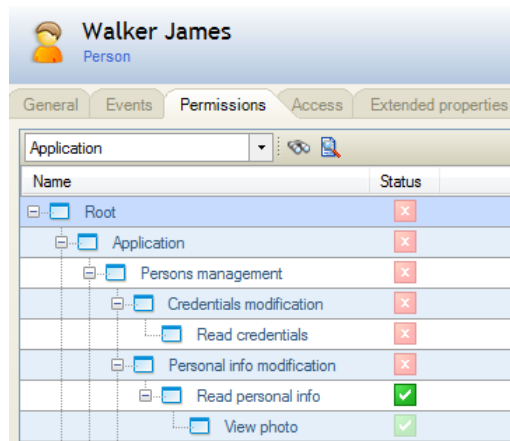


Figure 3-80 Person permissions for the Contact tab

After setting this permission, when Walker next logs in into the application with his account, he will see the *Contact* tab that pertains to him. He has no permission to view any data in the *Persons* tree except his own, because he has not been set any permissions for the *Persons* tree yet. This is the default set of permissions after creating an *Account*.

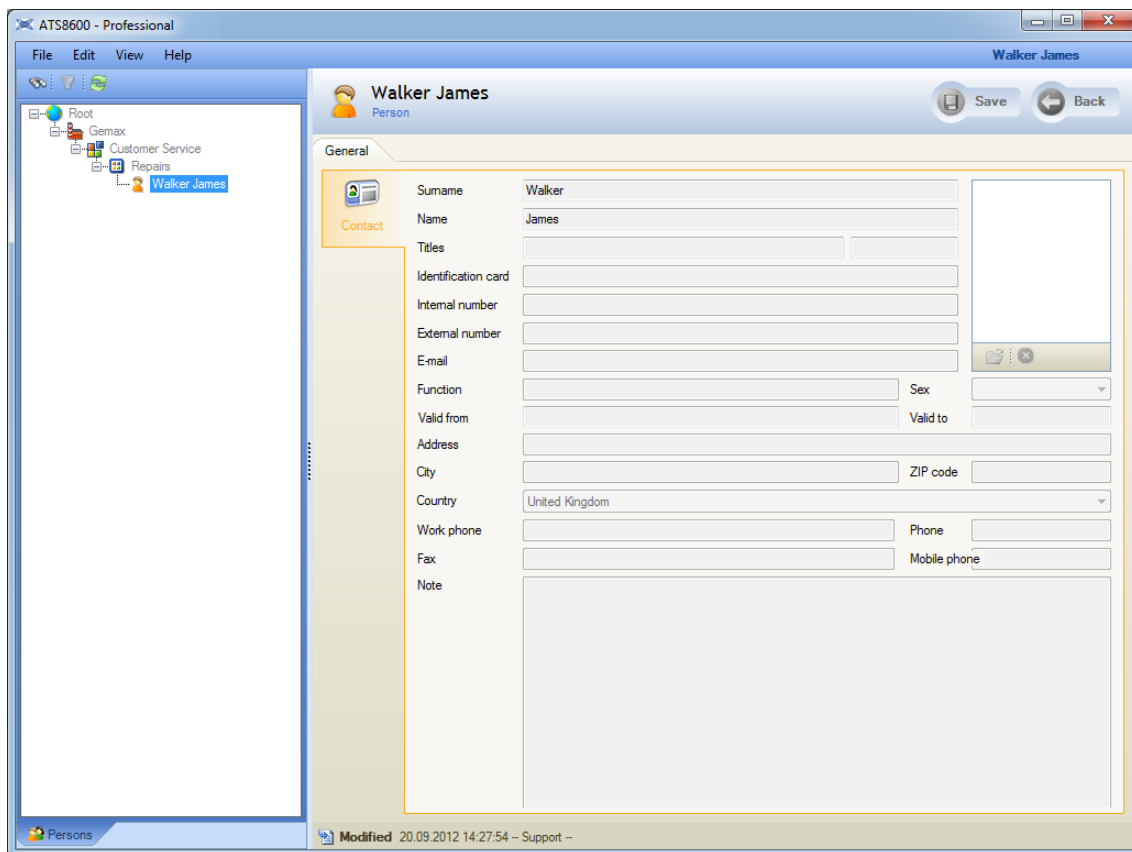


Figure 3-81 Permissions for the Contact tab

Now extend the *Application* permissions for Walker and enable all tabs of the *User management*.

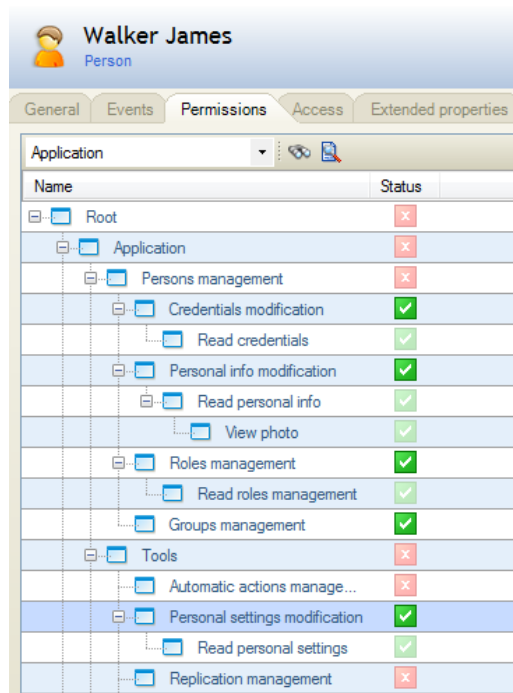


Figure 3-82 Setting read-only permission for all tabs of the Persons tree

After Walker has logged into the application with his account, the application window includes all enabled tabs. As in the previous step, he still sees only himself in the *Persons* tree. So he needs to be set permissions for persons.

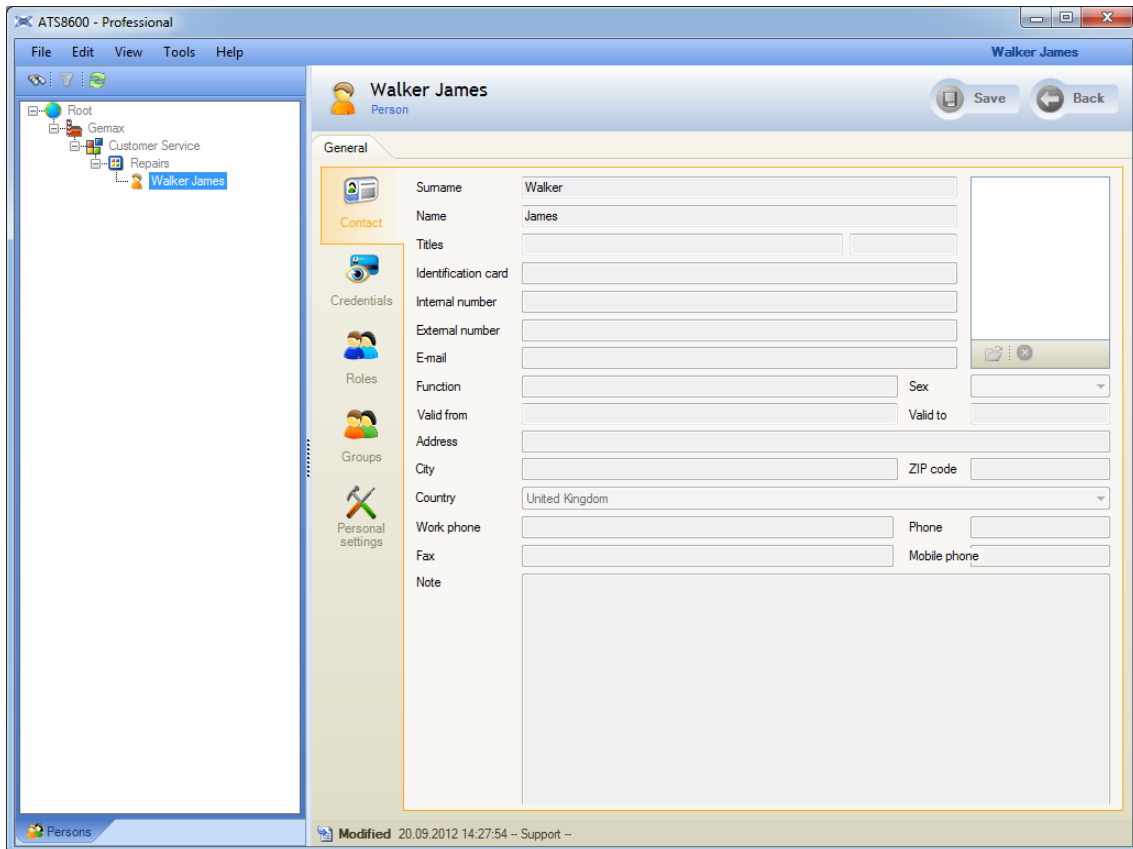


Figure 3-83 Read-only permission for all tabs of the Persons tree

5. Setting permissions for *Persons*

By setting permissions for *Persons* (permission group - *Persons*), Walker will be able to see information about *Persons* in enabled tabs for which he has permission.

Right-click the permission to grant Walker the permission to view the entire Service centre, and save the change.

Persons					
Name	Create	Read	Edit	Delete	Permissic
Root	x	x	x	x	x
Support	x	x	x	x	x
Gemax	x	x	x	x	x
Customer Service	x	✓	x	x	x
Receiving Order	x	✓	x	x	x
Clark Carolina	x	✓	x	x	x
Lewis Sandra	x	✓	x	x	x
Repairs	x	✓	x	x	x
Edwards Martin	x	✓	x	x	x
Miller Henry	x	✓	x	x	x
Walker James	x	✓	x	x	x

Figure 3-84 Assigning permissions for *Persons*

This permission allows Walker to view a part of the OS in the *Persons* tree - the Service centre.

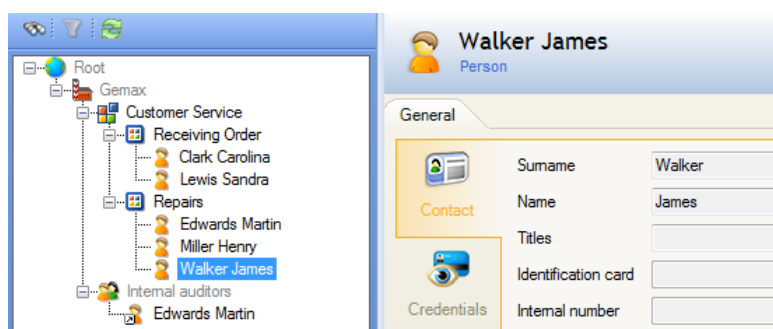


Figure 3-85 Read Persons permission result

As the previous figure shows, once Walker has logged in, the permitted part of the organizational structure appears in his *Persons* tree. However, because he only has view permissions, data in tabs on the right side of the screen can only be viewed, not modified.

If Walker's job includes the authority to edit or add persons' data, it is necessary to assign him the permission to edit persons. Select the *Edit* permission type and enable permissions to Walker for the Service Center.

Persons				
Name	Create	Read	Edit	
Root	☐	☐	☐	
Support	☐	☐	☐	
Gemax	☐	☐	☐	
Customer Service	☐	☒	☒	
Receiving Order	☐	☒	☒	
Clark Carolina	☐	☒	☒	
Lewis Sandra	☐	☒	☒	
Repairs	☐	☒	☒	
Edwards Martin	☐	☒	☒	
Miller Henry	☐	☒	☒	
Walker James	☐	☒	☒	

Figure 3-86 Edit permissions for Persons

Permissions		
Application		
Name	Status	
Personal info modification	☒	
Read personal info	☒	
View photo	☒	
Roles management	☒	
Read roles management	☒	
Groups management	☒	
Tools	☐	
Automatic actions manage...	☐	
Personal settings modification	☒	
Read personal settings	☒	

Figure 3-87 Permissions for Application must be allowed

When Walker logs in after this change, he has permission to edit data concerning persons in the individual tabs of the application window of the *Persons* tree.

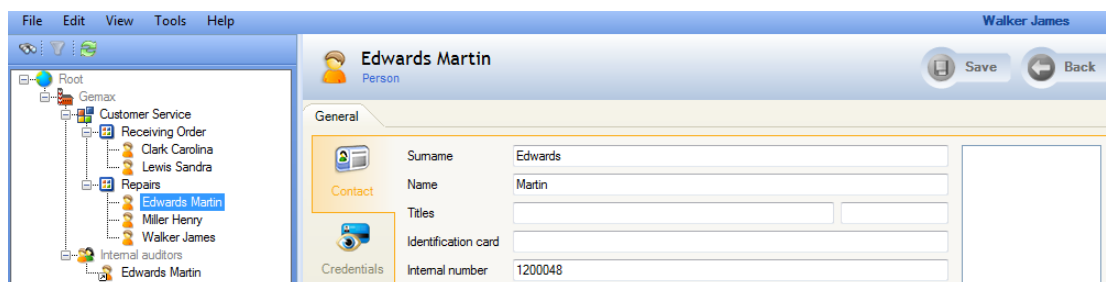


Figure 3-88 Permission to edit

6. Permissions for *Devices*

Previously, Walker did not have any permissions set for devices. Accordingly, she cannot see the *Devices* tree tab in the application window.

Note:

Sometimes it is not necessary for users to be able to access devices. For example, personnel department employees only require those permissions shown in the example of James Walker. An employee needs access to the organisational structure to view data concerning respective employees and, if necessary, even edit their contact information.

For technical workers, dispatchers, etc. it is necessary to set the permission in such a way that it is possible to work with devices. In order to do this, it is necessary to add the application rights for users (so that users can see the *Devices* tabs) as well as the rights for particular devices, which will subsequently be displayed in the *Devices* tree.

Click to select the person for whom you want to add permissions (James Walker) and open the *Permissions* tab. Select the *Application* permission group type and allow access to *Device Management*.

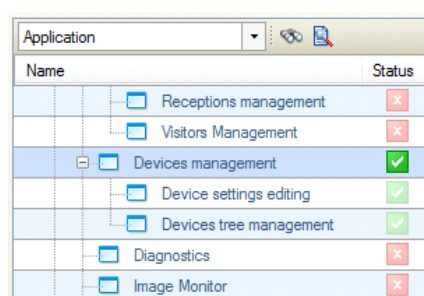


Figure 3-89 Allowing access to Device Management

If it is necessary for Walker to have permission to make changes in devices, permissions should also be set for *Device Management*. If it is sufficient for the user to view devices, allow only *Device settings*. The permission level is apparent from its description (e.g., management, editing, viewing).

However, after Walker's login into the application, the *Devices* tree tab will not be displayed in the window. To display the tree tab it is necessary to have permission for at least one device.

The administrator must enable permissions for *Devices*. In the permission group field, the administrator selects *Devices* and sets the required permission for the selected user (Walker). If a user needs only to view the permissions, choose Read permission.

If the user needs to modify device data, it is necessary to set the *Edit* permission for *Devices*. Enable permission for editing devices using the same method.

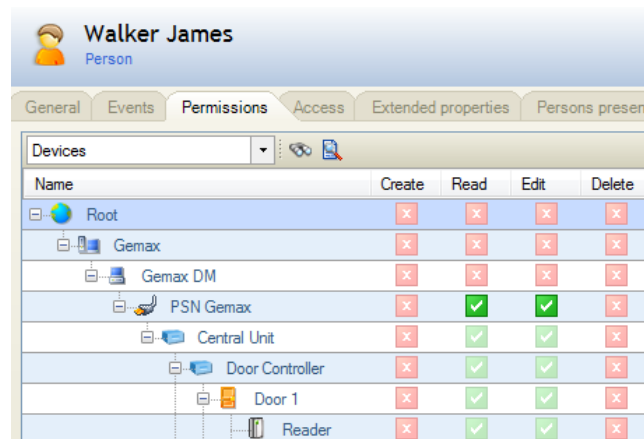


Figure 3-90 Setting the view and modify permission for Devices

Click **Save** to save permission settings and click the respective icon to refresh the application. After the next login to Walker's account, the *Devices* tree with allowed access appears on the screen in the *Devices* tab. In the right part of the window the user can view and edit details concerning particular devices.

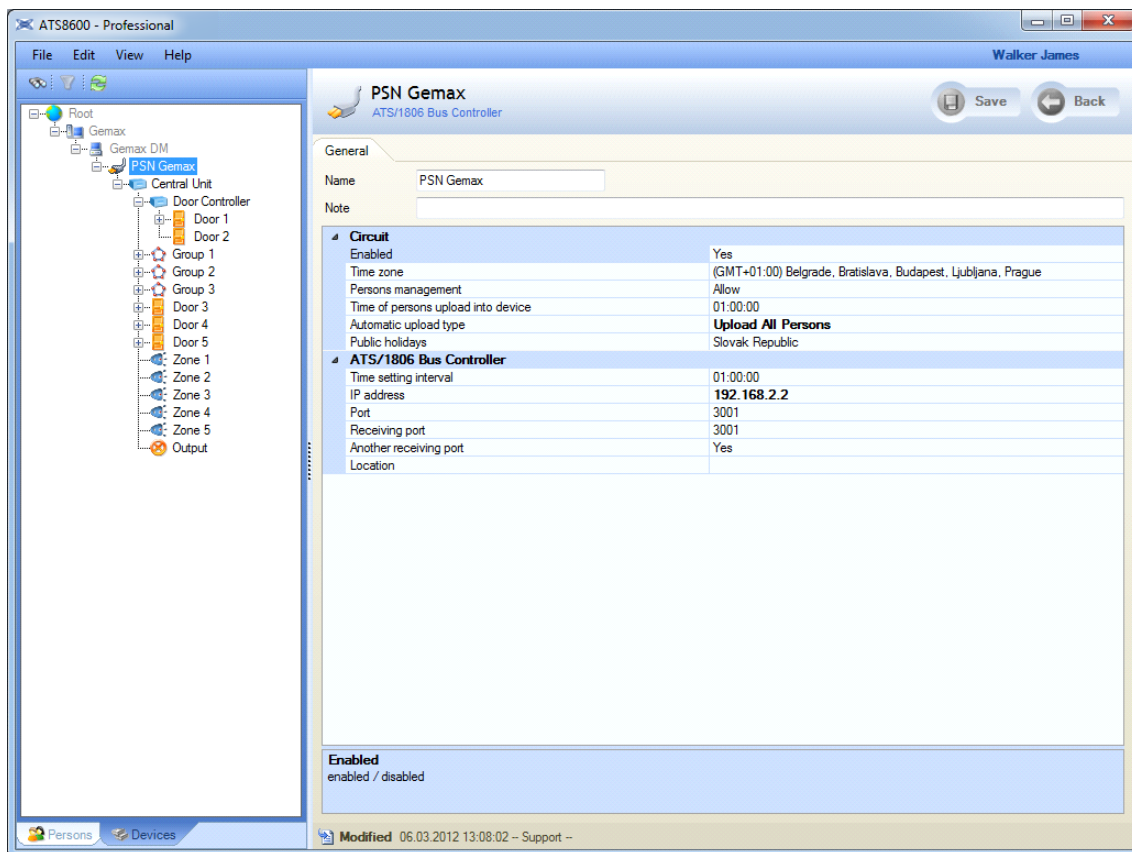


Figure 3-91 Devices tree

7. Setting permissions for *Events*

Events concerning persons and devices recorded by the system are displayed in the *Events* tab. If Walker needs permissions for events concerning certain persons or devices, permissions must be set:

- In the Application permission group, provide Walker with *Event History* permissions. This would display the *Events* tab in his window after login.
- The *Events* permission group includes the list of all monitored system events. In this permission group, enable permissions for Walker for particular events so they can be monitored in the *Events* tab after login.

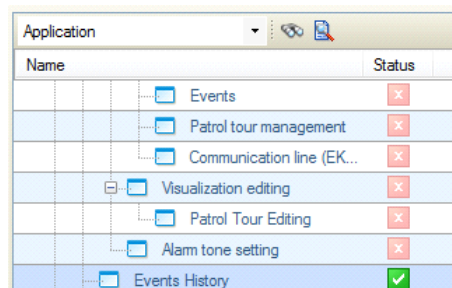


Figure 3-92 Allowing permission for the *Events* tab

Name	Read	Permissions
Root	X	X
Access events	X	X
Access allowed to [%PERSON%]	X	X
[%PERSON%] entered [%REG...]	X	X
[%PERSON%] left [%REGION...]	X	X
Access granted for unknown cr...	X	X
Access granted to [%PERSON%]	X	X

Figure 3-93 View only permission for Events

In order for Walker to display individual event filters in his *Events* tab, it is necessary to assign him with permissions for these filters. In the *Event filters* permission group, allow required permissions for available event filters. This will display the allowed event filters in his tab after login.

Name	Create	Read	Edit	Permissions	Delete
Root	✓	✓	X	X	X
Activities on devices	✓	✓	X	X	X
Access events	✓	✓	X	X	X
Device activities	✓	✓	X	X	X
Device settings changes	✓	✓	X	X	X
Alarms	✓	✓	X	X	X
Fire alarms	✓	✓	X	X	X

Figure 3-94 Event filters permissions

After login to Walker's account, the *Events* tab will be displayed with particular allowed events. The drop-down menu will contain only those event filters that Walker is permitted to view. If the person is permitted to edit the currently viewed event filter, the button next to the drop-down menu will be activated. For a description of filter editing, [see chapter Event filtering](#).

Walker James
Person

Save Back

General Events Permissions Access Extended properties Persons present Automatic actions

All activities

Time	Event
08/03/2013 17:55:17	User "Walker James (Repairs)" (192.168.1.8) logged on to ATS8600.
08/03/2013 17:22:21	User "Walker James (Repairs)" (192.168.1.8) logged out of ATS8600.

Figure 3-95 Events in application with the possibility to edit the event filter

Warning:

After changing the user's permissions of the client application, it is necessary to restart the client application of the user whose permissions have been changed.

3.7 Access

The *Access* tab on the navigation panel provides information on whether an OS object (company, department, center, person) is granted access rights to particular devices or regions.

Since information on the allowed access to devices is very frequently requested, clicking **Access** provides this information immediately.

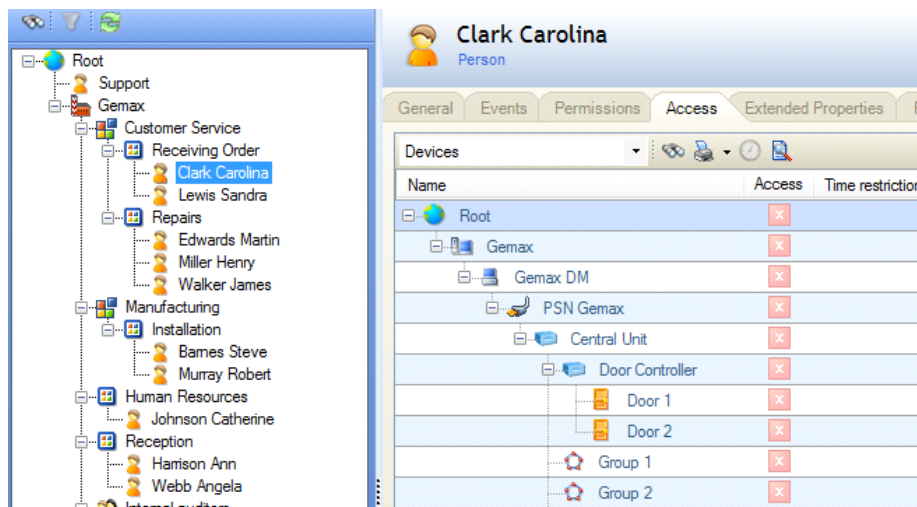


Figure 3-96 Access tab

To learn more about the Access rights permission states, see [the chapter Permission state](#).

3.7.1 Allowing access to devices

In the **Access** tab, an authorised user can set the access to devices for persons. In the *Persons* navigation tree, select the person whose access you want to edit. In the **Access** tab search for the device for which you wish to edit the access. Right-click the status and select the **Allow** status.

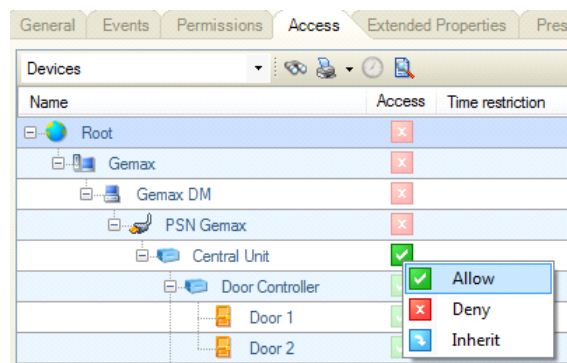


Figure 3-97 Allowing access to a device

3.7.2 Allowing access to regions

In the **Access** tab, an authorised user can set access for different persons to devices in certain regions. In the *Persons* tree, select the person whose access you want to edit. In the **Access** tab, search for regions to which you want to grant access. Right-click and select the **Allow** status.

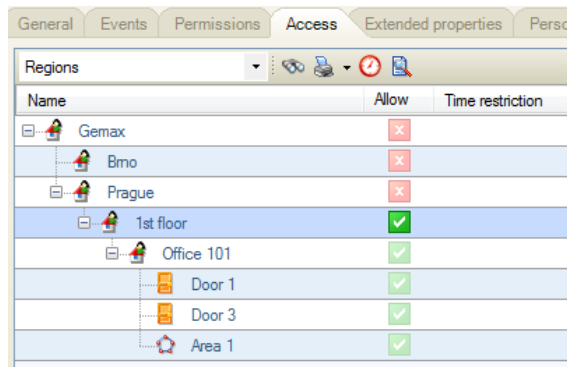


Figure 3-98 Allowing access to a region

3.7.3 Time Restrictions

By granting the *Access* permissions for *Devices* or *Regions* object, you can set a certain time restriction for the chosen OS item (e.g. a person). Restricted period means that a person is allowed access to a device/region (e.g., an access door) within a certain time period.

Setting a time restriction

1. In the *Persons* tree select the OS object for which you wish to set the time restriction.
2. On the right side of the screen open the *Access* tab.
3. Select a device/region with access allowed for which you want to set a time restriction.
4. Click  to set a time restriction. The icon is only active when access to the device is allowed.

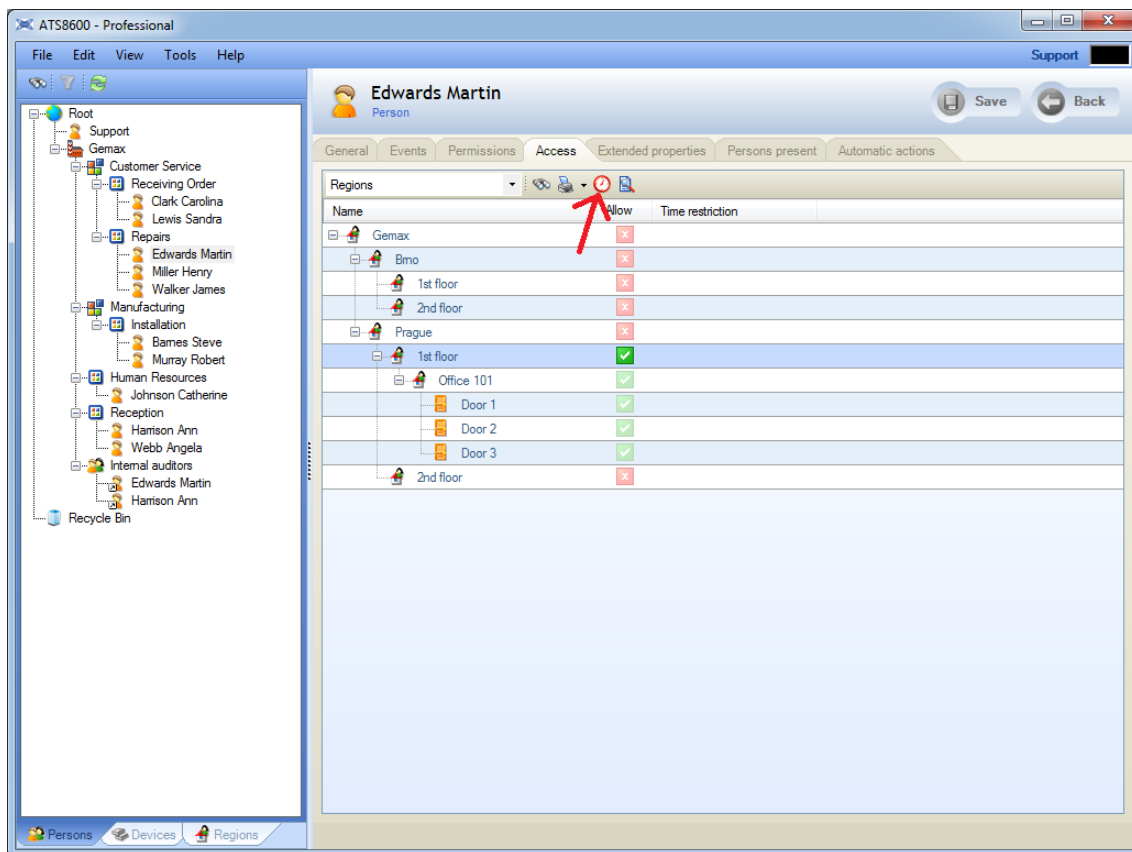


Figure 3-99 Setting a time restriction

Select **Edit** in the time restriction settings menu to open a window with graphical representation of restriction settings. In this window you can edit set restrictions, add more restrictions or delete existing restrictions for a person.

To define time restrictions for an access to devices or regions in the window in accordance with the following picture, do the following:

1. Click **Add**. Enter the name for the defined restriction in the upper left-hand corner of the screen (e.g., the name of the restriction like Working hours).
2. In the right part you can graphically mark the restriction duration. When moving the mouse in the network, at the bottom of the application window your current position (date and time) is displayed.
3. Enter the date range for which the restriction may be valid.
4. Click **OK** to confirm the setting.

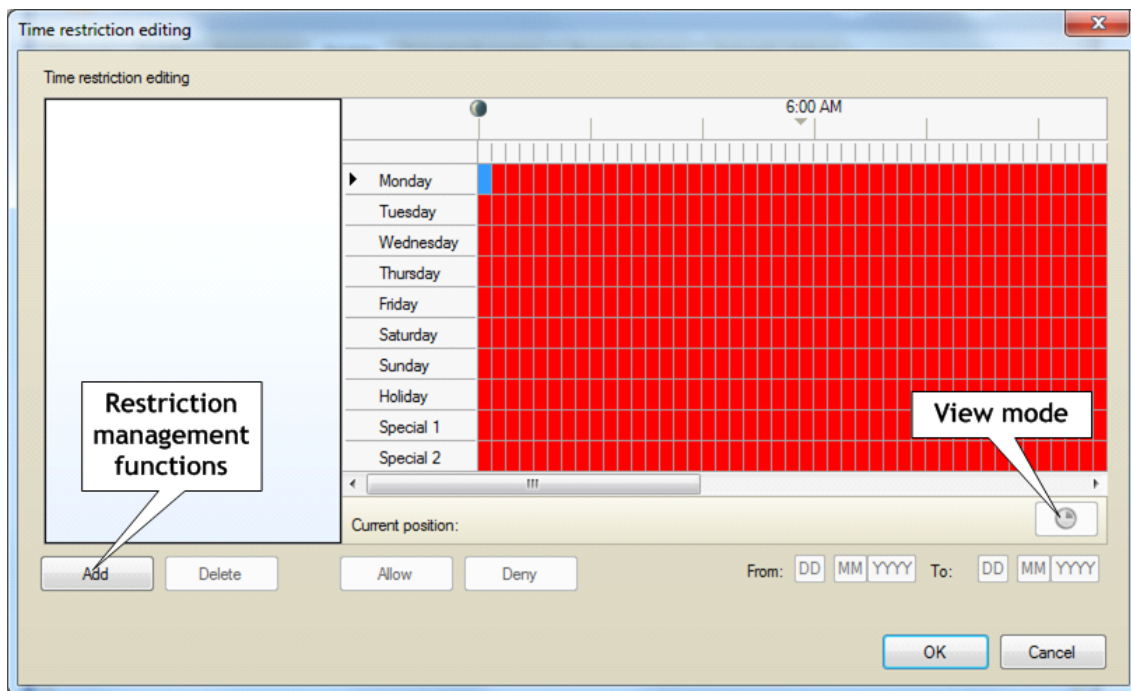


Figure 3-100 Graphical representation of a time restriction

Click  in the lower-right corner to switch the calendar view mode and display a graphical visualisation of time restrictions.

There are two modes of calendar visualization

- With quarter-hour intervals (default setting)
- With hour intervals

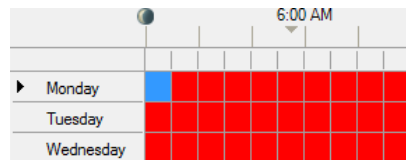


Figure 3-101 Calendar view with hour intervals

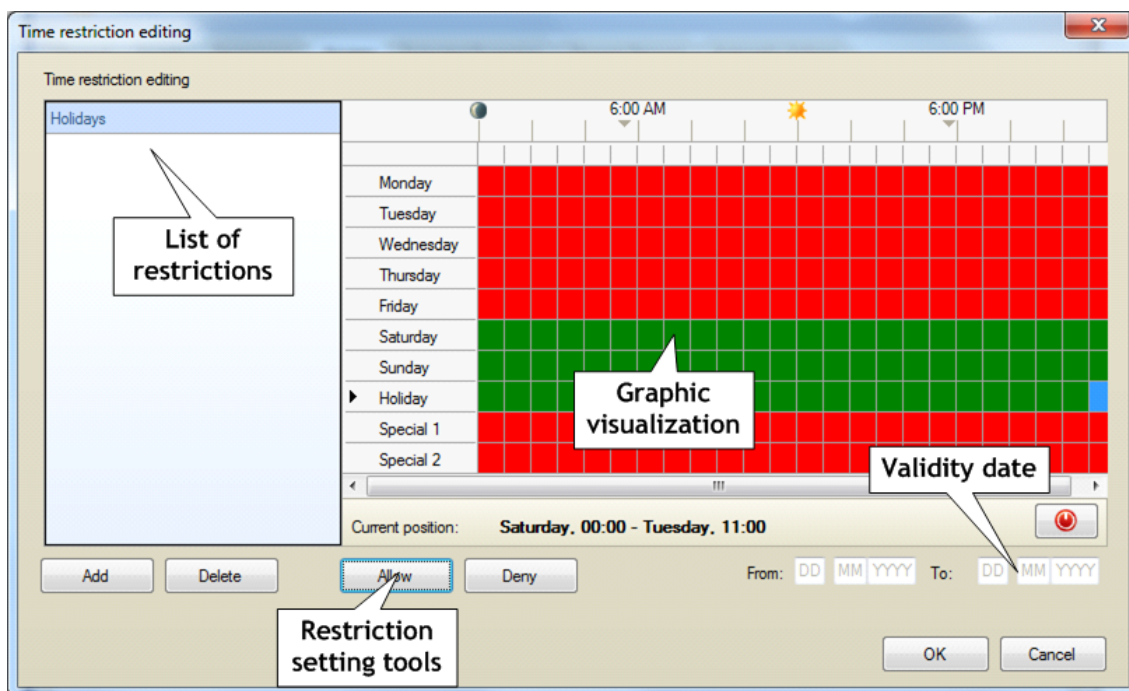


Figure 3-102 Time restriction set

Office 101	✓	Holidays
Group 1	✓	Holidays
Door 1	✓	Holidays
Door 3	✓	Holidays
Door 4	✓	Holidays

Figure 3-103 Time restriction setting icons

The validity dates for the time restriction can be set in the from and To fields. Outside the set dates, the time restriction is ignored and the access is considered as denied.

Note:

By creating a new permission no time restriction is automatically set.

Note:

The time restriction can be set only for restricting access in the *Access tab*.

Note:

The row "Holiday" represents non-working days, which are defined separately for each country (see [Holidays](#)).

3.7.4 Holidays

Holidays and non-working days are important for access management, therefore they must be defined correctly. On each device supporting access management holidays are considered according to the country set in properties of this device in the device tree. The easiest way of defining holidays is loading from a file (see [Import of Holiday Definition from a File](#)). If such a file is not available, the system allows to edit the holiday definition manually (see [Entering Holidays Manually](#)).

3.7.4.1 Import of Holiday Definition from a File

The holidays definition can be loaded from a *.hol file, which is part of the Microsoft Outlook installation, or can be downloaded from the internet as a separate file.

1. From *Tools* menu open the *System settings* panel - *Holidays*. Select the country which holidays you want to import.

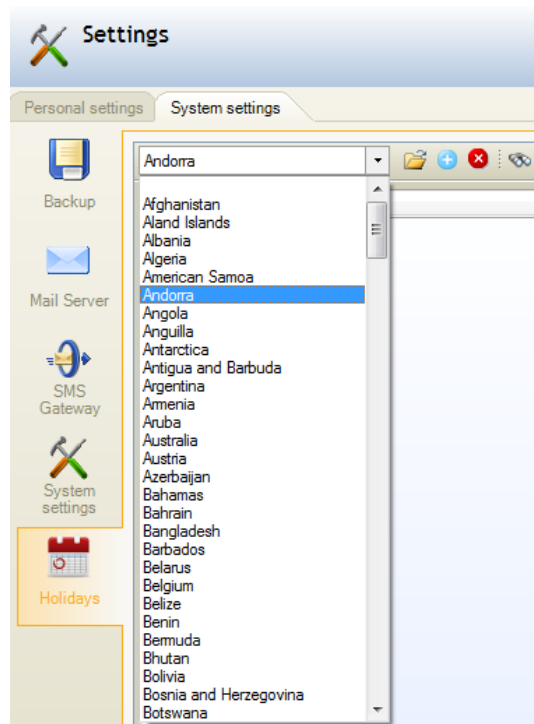


Figure 3-104 Selecting a country

2. Click  to open the dialog box. Browse for the .hol file, which contains the definition of holidays of the required country.

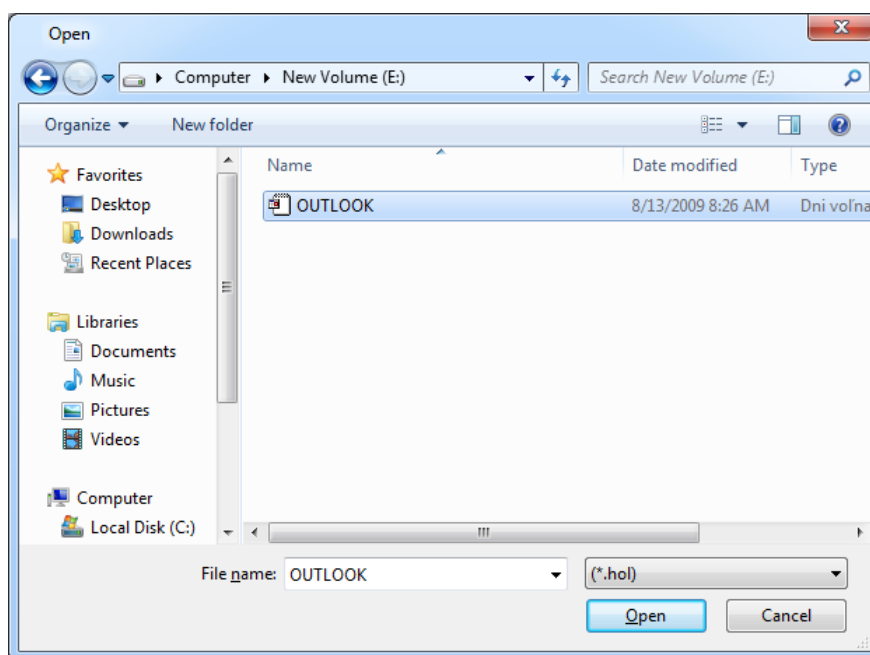


Figure 3-105 Selecting the imported file

3. If the selected file includes definitions for multiple countries, select the country which holidays you want to import.

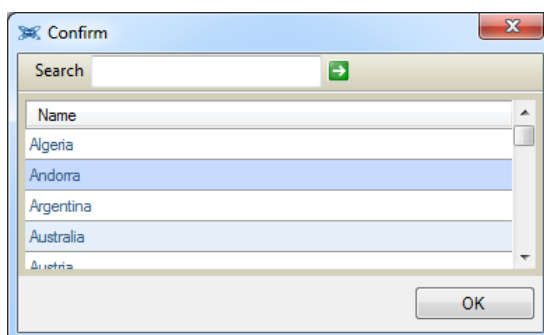


Figure 3-106 Selecting a country

4. After successfully importing the definition from the file, all holidays of the respective country for the upcoming period will be shown in the list.

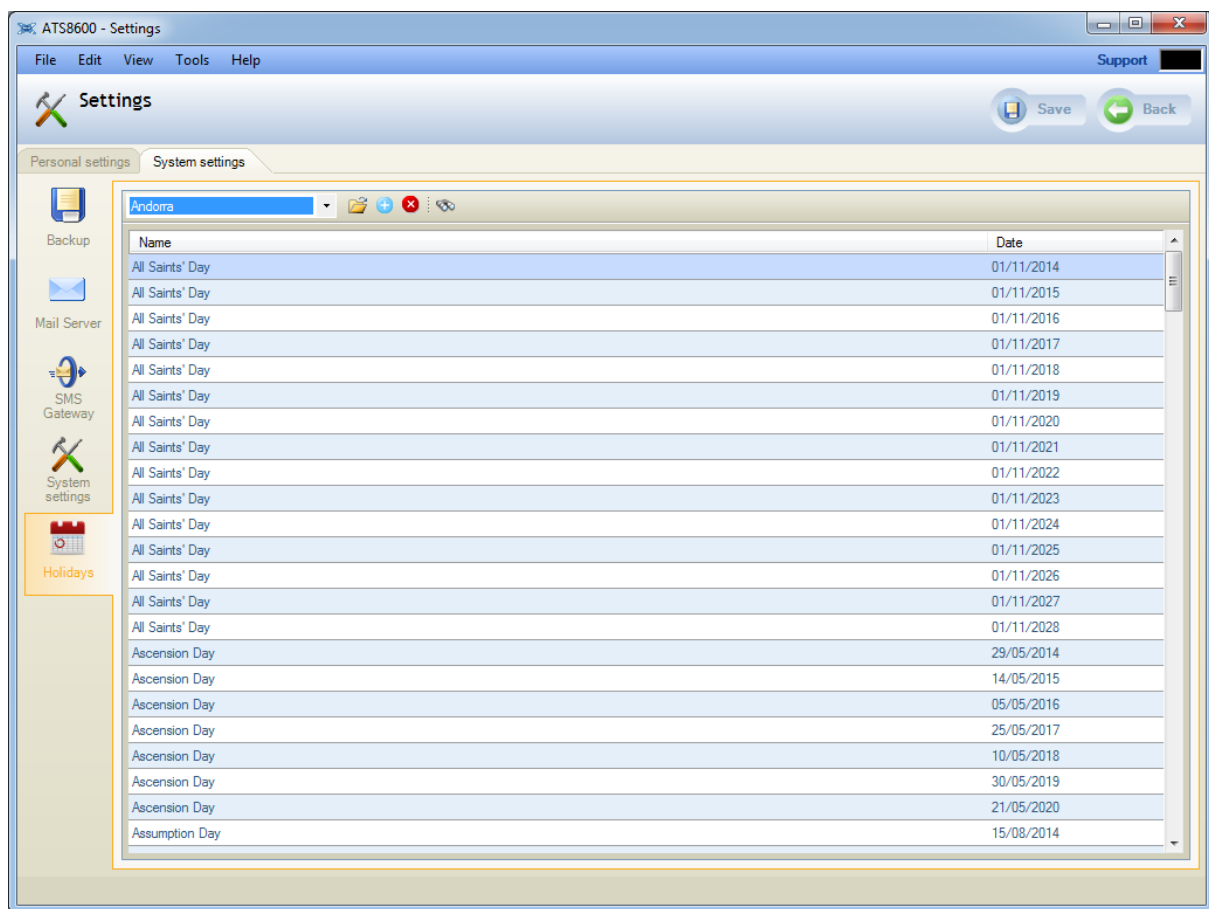


Figure 3-107 Definition loaded from a file

5. If you need to manually edit or add holidays, follow the steps in [Entering Holidays Manually](#).

Warning:

Changes made in the holiday definition will take effect on the device only after the next successful upload of identifiers.

3.7.4.2 Entering Holidays Manually

1. Select the country which holidays you want to edit.
2. Click  to add a new line to the line list.
3. Enter the name of the holiday.

St. Carlos Borromeo
Custom Holiday

Figure 3-108 Naming a holiday

4. Select the date of the holiday.

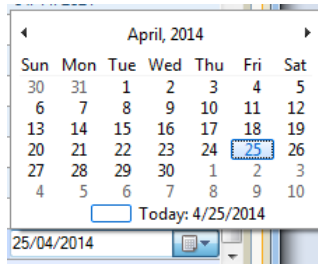


Figure 3-109 Selecting the holiday date

Note:

Click  to delete an unnecessary row.

3.7.5 Access report

To create a report on access rights granted for individual devices or regions in a very quick way. The report can be printed later. Click the  icon to select the function for generating the report. The report provides an overview of where and to what devices/regions the person has access.

The user can generate a report in two ways:

- Print all access permissions to access points
- Print only allowed access permissions to access points

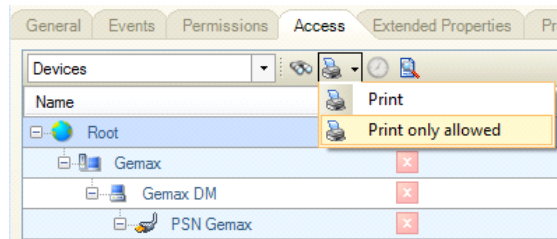


Figure 3-110 Print access permissions

Access						
	Door 1 (Door Controller)	Door 2 (Door Controller)	Door 3 (Central Unit)	Door 4 (Central Unit)	Door 5 (Central Unit)	Group 1 (Central Unit)
Clark Carolina (Receiving Order)	✓	✓	✓	✓	✓	✓

Figure 3-111 Report of all access permissions to devices of a person

Access					
	Group 3 (Central Unit)				
	Door 5 (Central Unit)				
	Door 3 (Central Unit)				
	Door 2 (Door Controller)				
	Door 1 (Door Controller)				
Clark Carolina (Receiving Order)					
		✓	✓	✓	✓

Figure 3-112 Report of granted access permissions to devices of a person

Note:

The generated report contains access permissions of a currently selected device and its child nodes.

4 Extended properties

Extended properties follow the previous chapters dealing with *Permissions* and *Access*. Permissions define the allowed functionality for the user in the ATS8600 Integrated Security Management System. Access defines to which devices the user can apply the functionality. Describe a more complex security framework of a particular person for devices on ATS8600. In other words, it specifies the settings and rights that the person has within a particular device.

For example the possibility to enter the PIN on devices is defined in *Access*, but other specific rights for this device are defined in *Extended properties*.

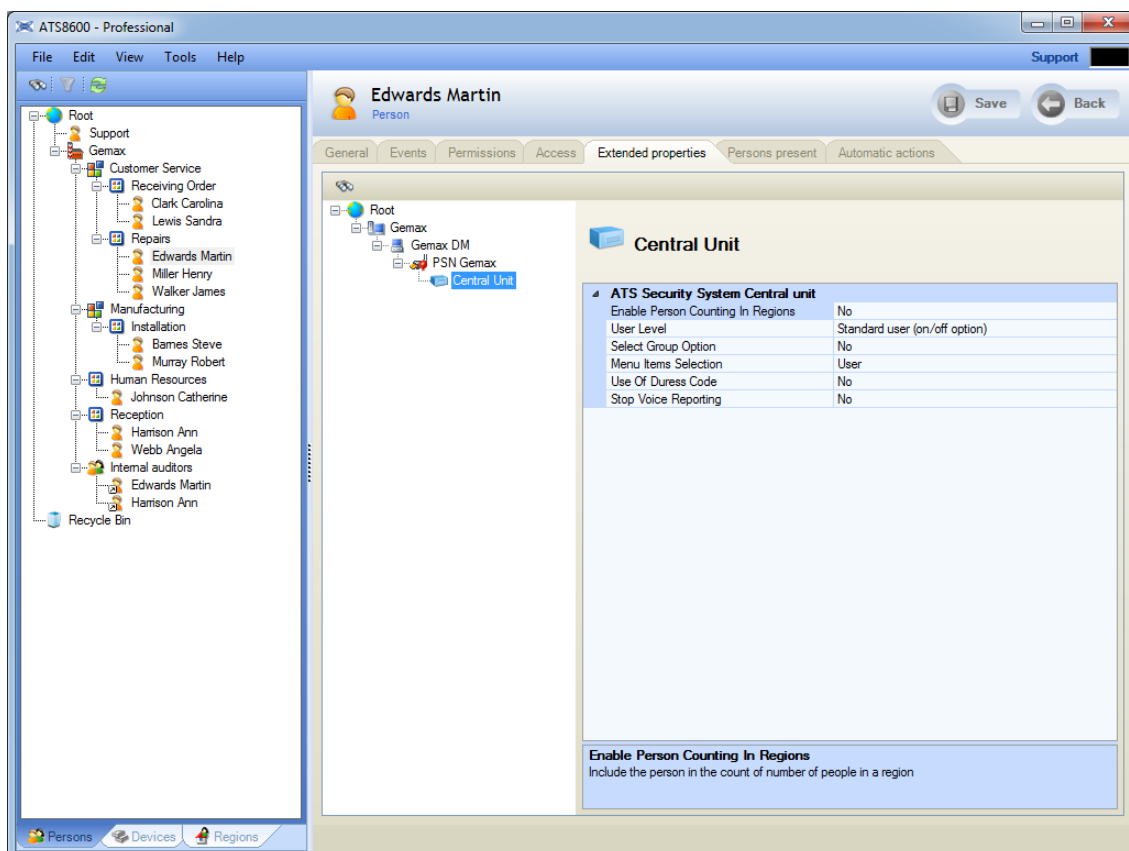


Figure 4-1 Extended properties

The extended properties setting is based on the principle of inheriting, similar to that of *Permissions*. The inheriting principle is described [in chapter Principle of inheriting](#). Extended properties can also be set on objects in the *Persons* tree, as well as on receptions and corridors in the visitor module.

5 ATS8600 Device Manager

In case of a primary ATS8600 server failure (or connection loss), the administrator can start a so-called secondary server. There is no need to configure the secondary server, as all services are ready for use. For each ATS8600 service (*Message Broker*, *Device Manager*, *Replication Manager*) the primary (default) and the secondary MAC (HW) Address can be set by the administrator.

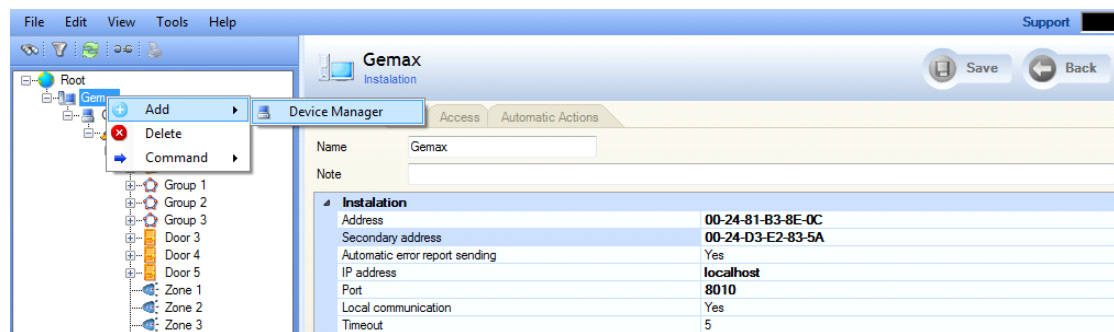


Figure 5-1 Secondary server set-up

6 Device Management

The *Devices* tree provides a complex management of devices and technologies used by the ATS8600 Integrated Security Management System. Individual devices are displayed in the tree in a hierarchical structure as implemented in the system.

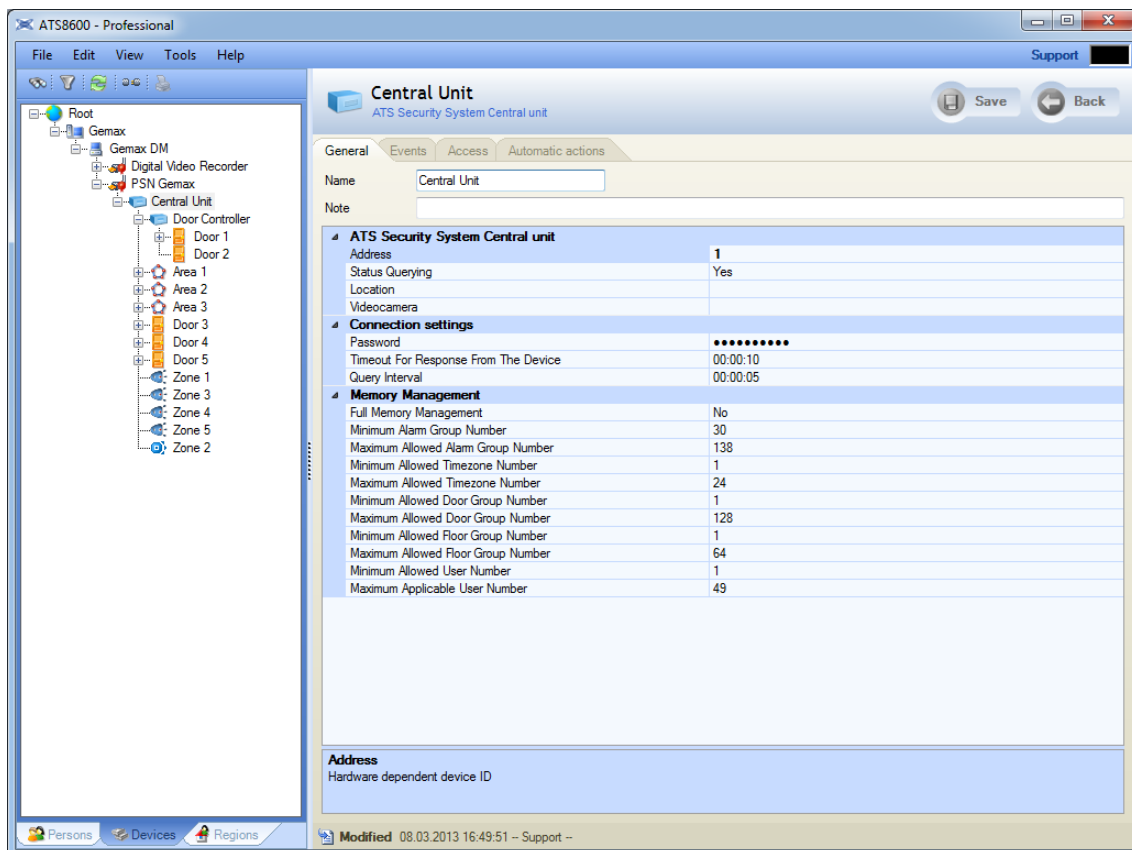


Figure 6-1 Devices tree

The structure of the *Devices* tree is similar to the *Persons* tree. In the tree you will find a list of devices for which the user has been granted at least minimal access. You can view data about the device by clicking the respective device. Its settings will then appear on the right. The bottom part of the window displays brief information about individual settings.

6.1 Adding a device

The system of adding a device to the tree depends on the menu, which is displayed after right-clicking the object to which you wish to add the device.

Adding an object type to a particular location is not random. The system contains controlled support for the hierarchy; that is, the system controls what type of object can be created at the given node of the navigation tree. This will be apparent in the function menu when creating a new object.

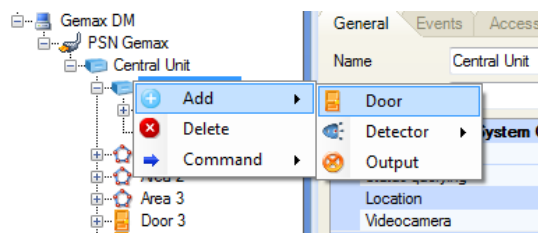


Figure 6-2 Selecting a function in the Devices tree

After selecting a command a window will pop-up in the right part of the screen. It might be necessary to enter some information

- **Name**
 - enter the name of the added device
- **Note**
 - enter a note you want to keep in mind
- **Address**
 - address of the device; the way of addressing depends on the particular connected device and how it is explained in the respective integration manual.
- **Location**
 - information about the location of the device
- **Camera**
 - camera in whose field of vision the device is located ([see chapter Searching for video records with events](#))

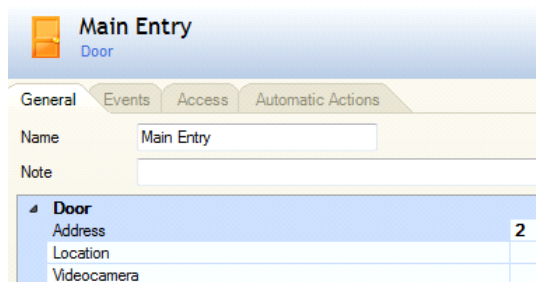


Figure 6-3 Entering device information

Note:

For more information on working with objects and calling functions, [see chapter Working in the Professional view](#).

6.2 Running a device

In order to establish communication between the new device and the ATS8600 Integrated Security Management System, it is necessary to start a communication circuit of the given device. Initiate this communication by right-clicking the device's bus controller and clicking **Run**.

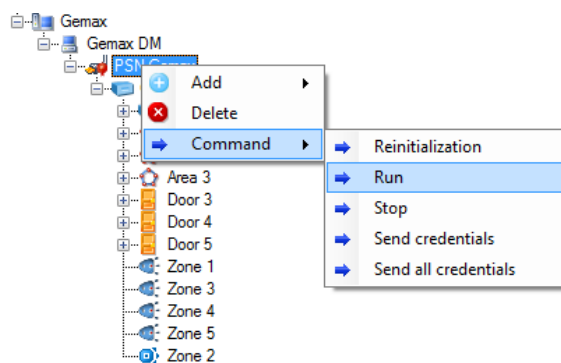


Figure 6-4 Running a circuit

Stop the communication with the device by clicking **Stop**. **Reinitialization** makes it possible to stop and start communication with the given device.

Warning:

If the user changes the configuration of any device in the *Devices* tree (e.g., change in addressing, login data, etc.), it is necessary after saving these changes to stop and start the corresponding circuit in order for these changes to manifest in the communication with the given device.

6.3 Changing the device type

In the *Devices* tree, each device is represented with an icon that characterizes it visually. It is possible to change the category of some elements by right-clicking the selected node in the device tree and selecting **Change type**. For example, in case of detector elements it is possible to change one type of the detector with another type from the list.

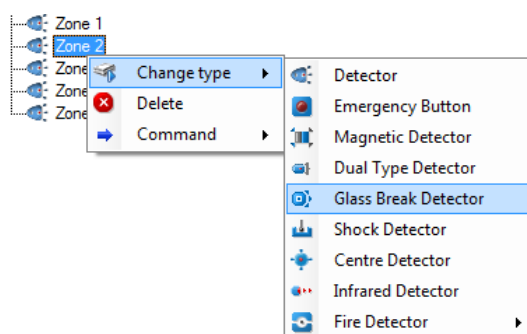


Figure 6-5 Change of the detector type

To perform this operation, the logged-in user must have permissions to view and edit the selected device. When the element type is changed, all its properties and events that were created on this element prior to the change will be kept.

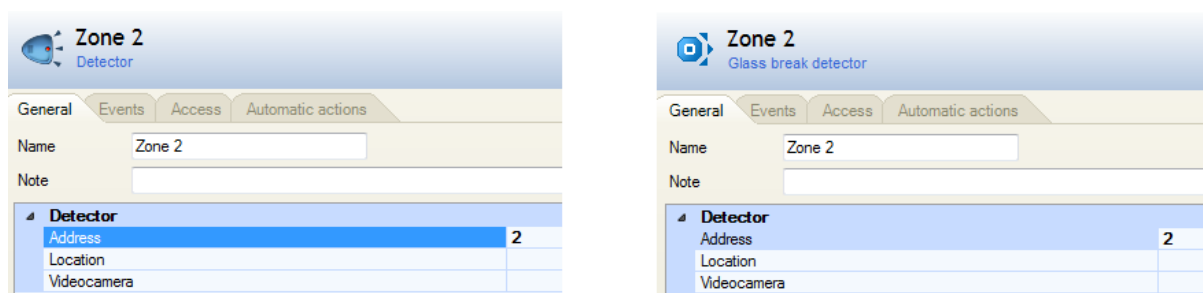


Figure 6-6 Detector's properties before and after the change of the type

Warning:

A change of the element type will be reflected on other ATS8600 clients only after their client applications are restarted.

For the proper functionality of the circuit, it is necessary to restart the respective circuit after the element type change.

6.4 Device statuses

The *Devices* tree includes the **Statuses on** command. Click the icon to switch between displaying statuses of devices and edit mode.

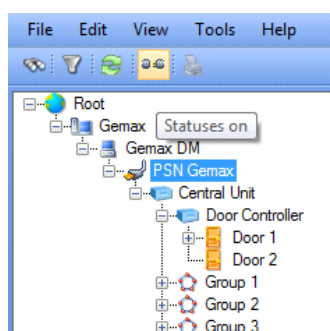


Figure 6-7 Status display

Monitoring mode - If displaying statuses is on, the devices icons reflect the real status of the devices. Active devices are displayed in color and inactive devices in grey. In this mode commands for devices can be issued (e.g. Disarm, Arm).

Status display ensures that:

- respective dispatchers check the actual status of particular devices. A change in device status is shown by the change of icon on the device. When the door is open, the employee can immediately see this in the application.

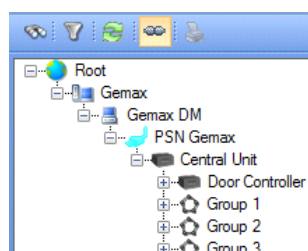


Figure 6-8 Active statuses

Edit mode - When statuses are turned off, icons are displayed in colour but do not reflect the real status of devices. In this mode the *Devices* tree can be managed (edit and/or a device can be deleted). In this mode commands for devices can be issued (e.g. Disarm, Arm).

6.4.1 Device statuses filter

It is possible using the device status filter to show only devices in a specific state. The acquired list can be printed out as a report.

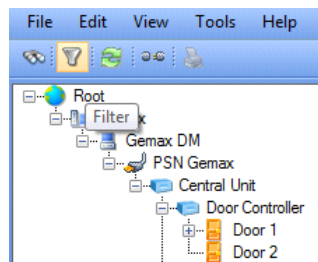


Figure 6-9 Device statuses filter

Devices in the required status are also represented graphically.

Example:

Devices with an unknown status are shown greyed out in the tree structure.

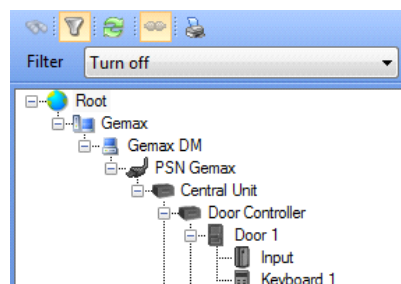


Figure 6-10 Filter applied to the tree

A specific device status is FPS daily control support. This filter includes the following statuses: Normal, Testing, Failure and Alarm.

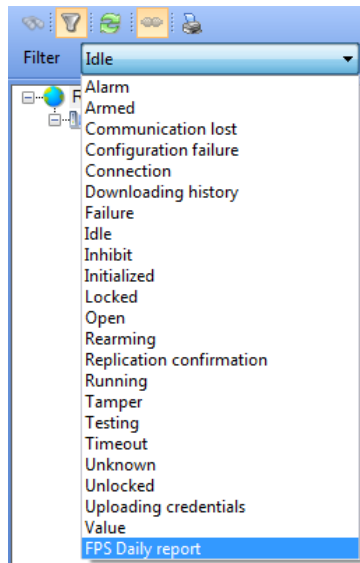


Figure 6-11 Filter items

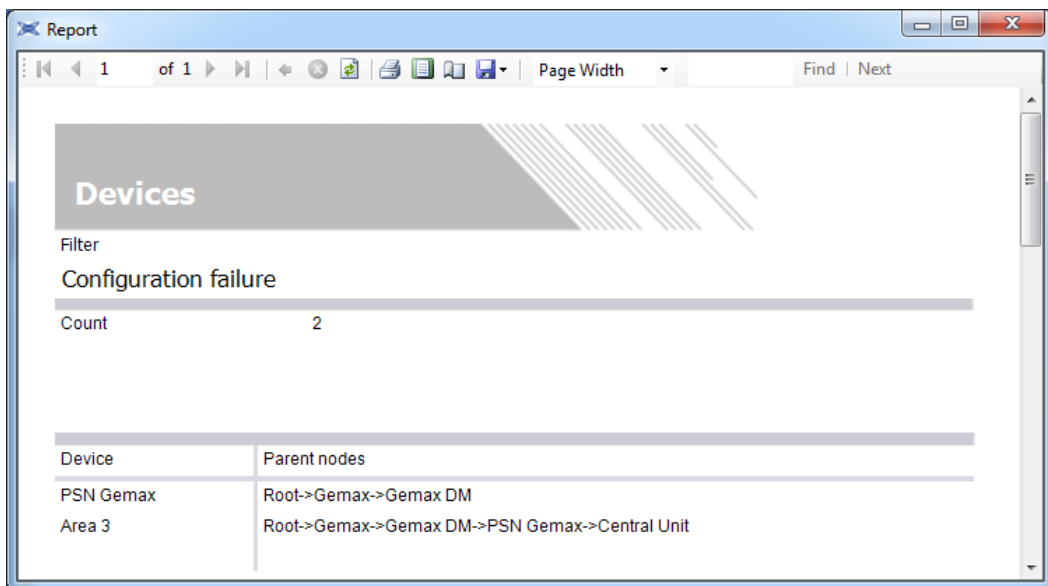


Figure 6-12 List of devices with a selected status that is ready for printing

This function is located in the *Regions* tree and in the *Monitor* panel. When using the filter in a specific region, you can set the initial group of devices. From this group, the filter is applied for this group.

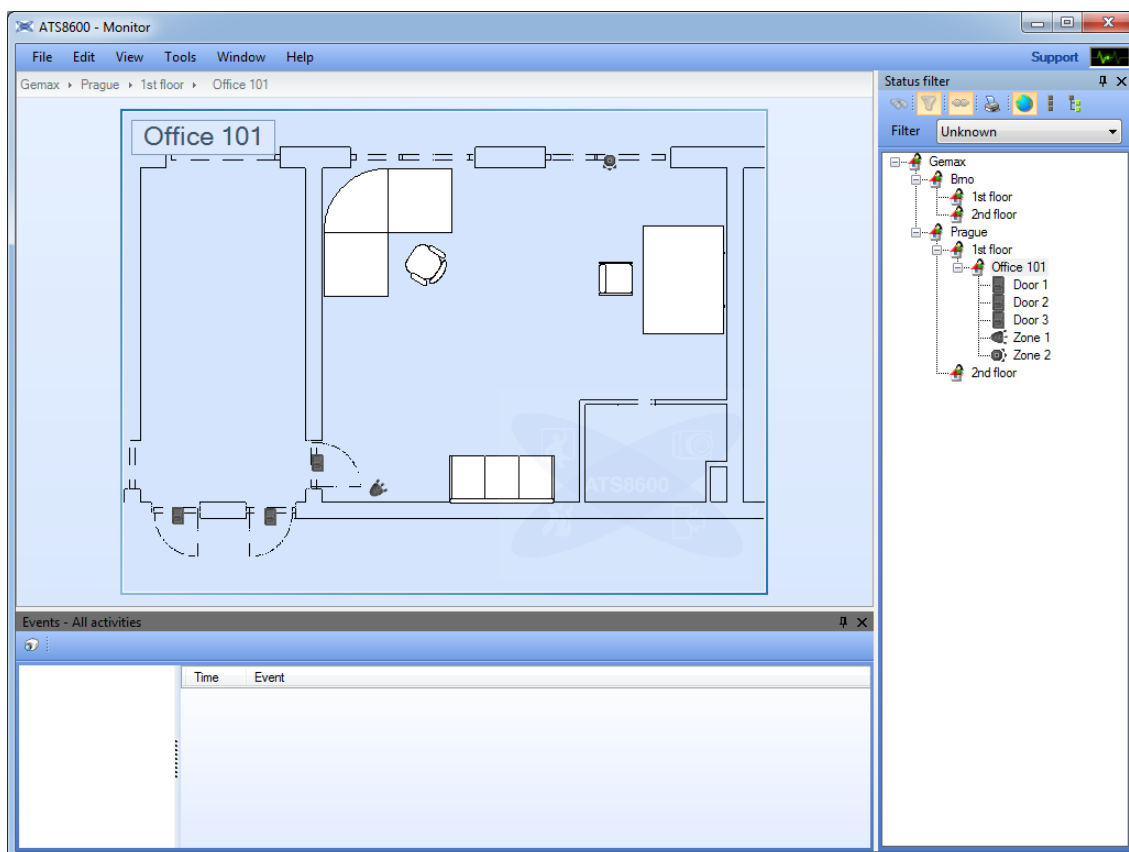


Figure 6-13 Device statuses in the Monitor panel

You can choose from the following three initial filter groups:

1. The whole tree *Regions* 
2. Devices in the current region 
3. Devices in the current region and its sub-regions 

In case you do not want to use only one region, select the Monitor full tree function. Then the device statuses filter filters the entire device tree.

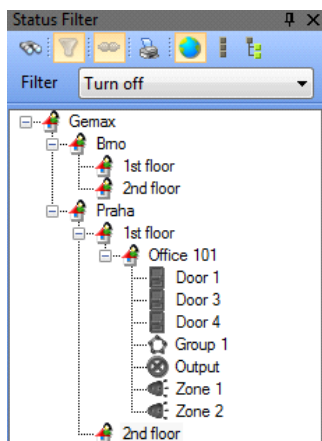


Figure 6-14 Monitoring a full tree

7 Regions

The *Regions* tree can be arranged as needed, but normally it reflects device locations grouped in a region.

A region is an area in a premise that contains all devices managed by ATS8600 in that area. A region reflects devices against an area of a building. It may contain different device types (e.g. inputs, outputs, camera's, etc) or device locations (e.g inputs from 2 different panels or camera's from 2 different video devices). In other words, ATS8600 Integrated Security Management System that disregards the number and location of the covered buildings and the number of devices included in the system.

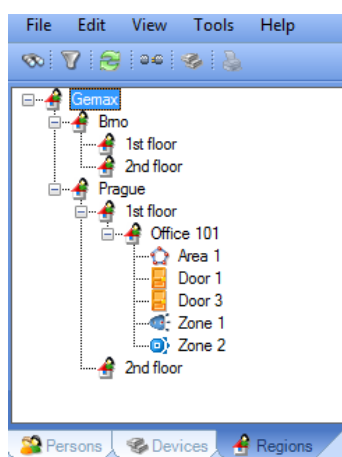


Figure 7-1 Regions tree

7.1 Create regions

The *Regions* module enables to create the main - Region structure, i.e. to create subregions, based on the real hierarchy level structure of superior and subordinate parts of the main - Region.

The tree structure begins in the main - Region, which is initially named After the computer running the ATS8600 server. In this example, it is called Gemax. Rename the region to the required name for your installation.

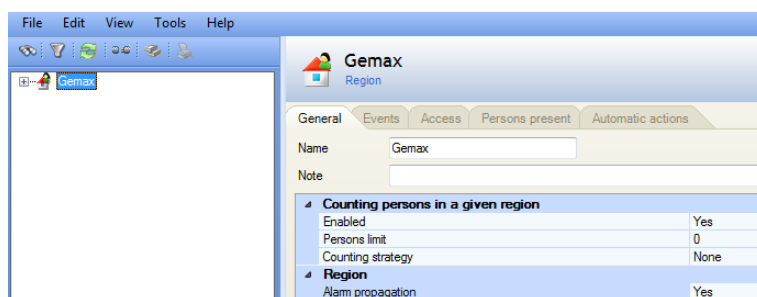


Figure 7-2 Main region Gemax

Then create a subregion structure from the main region according as required. To create a subregion, right-click the parent region and select **Add - Region**. You can also create a *Button* in the *Regions* tree, which can then be defined to perform an automatic action. After creating the button, you can

click it in the *Monitor* panel, which will then performing the automatic action. This functionality serves to manually execute commands from the *Monitor* panel (e.g., arming all areas, switching all output devices, etc.). A detailed method of adding the button to the system is described [in chapter Adding a Button in visualization](#). In the *Regions* tree, a *Label* can be created to serve as a user text description, which can be visualized on the ground plan of the respective region. The *Label* element does not support any commands or statuses; it only provides a text information for the user.

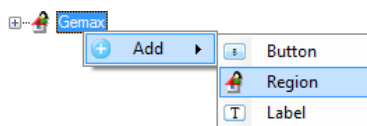


Figure 7-3 Creating a sub-region

Enter and save details of the new sub-region.

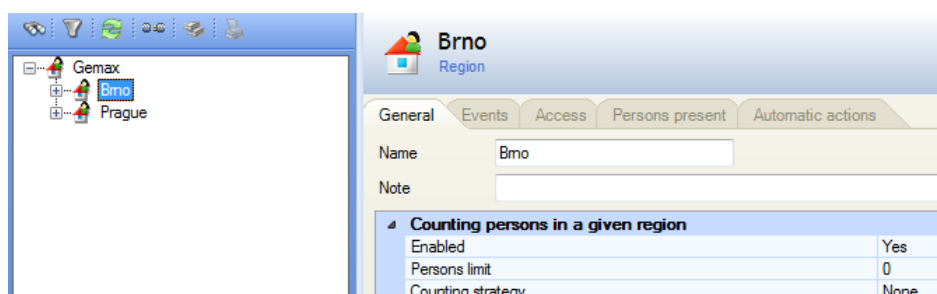


Figure 7-4 Entering region information

7.2 Device structure in a region

Apart from creating region and subregion structures the tree also allows allocation of individual devices in these regions when these devices are located in this region.

Therefore, it is necessary to add the devices defined into the *Devices* tree to individual regions.

To add the physical location of the individual ATS8600 device into the region structure, click *Devices* to display the *Devices tree*.

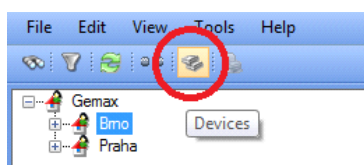


Figure 7-5 Displaying the tree Devices

The *Devices* tree will appear next to the *Regions* tree. To close the *Devices* tree, click again.

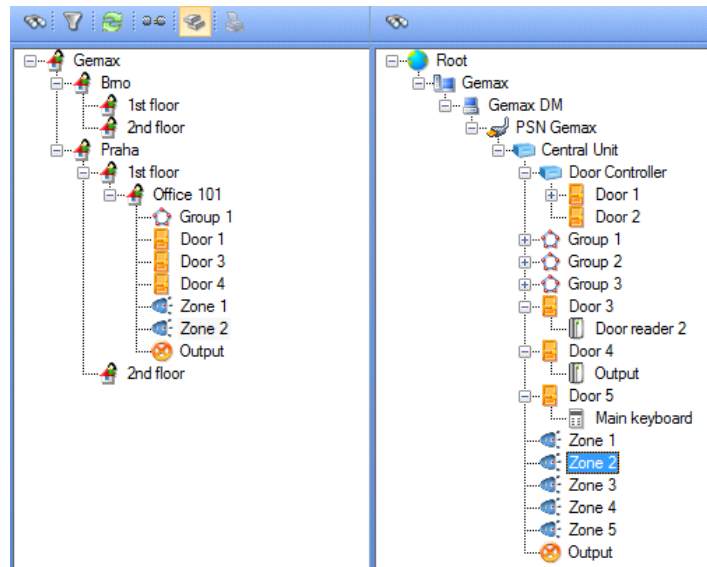


Figure 7-6 Devices tree (right)

From the device tree, drag & drop required devices into the given regions according to their location. The intention is for every subregion to include all devices that are present in the given area that is represented by the region.

Example:

Click and hold Door 5 and drag the cursor over the Office 101 sub-region, where the device is located. The cursor will change to . Then release the mouse button. The device has been added to the region.

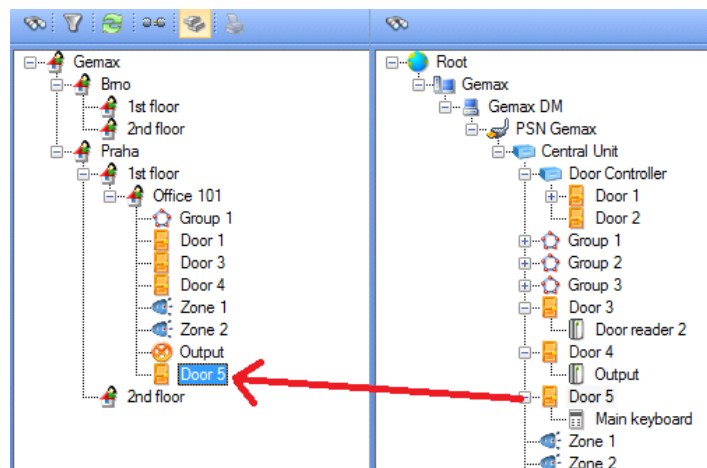


Figure 7-7 Drag & drop transfer of a device

Locate all devices into their subregions as described above.

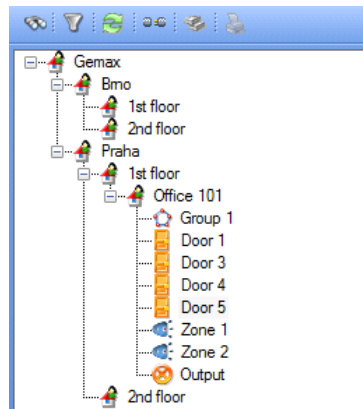


Figure 7-8 Devices structure of a region - Logical tree

Tip:

To move devices into regions, we recommend using the Visualization panel because it is more simple. Upon visualizing the device on the ground plan, the device is automatically positioned in the respective region ([see chapter Example of visualisation](#)).

In case you mistakenly added a device to a region or if you need to remove a device from a region, perform the following steps:

1. Right-click to highlight the device you wish to remove from the Logical tree.
2. Select the remove function to delete the device from the region.

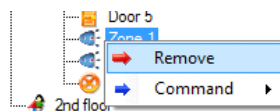


Figure 7-9 Removing a device from a region

Formatting the logical device tree in regions does not influence the *Devices* tree as this physical tree represents the technical connection of these devices and does not involve their spatial location.

It is possible to issue commands for some remotely controlled devices.

For example, It might be possible to open a set of doors not only in the classical way by swiping a card on a reader, but also remotely by sending a command from the application by an authorised user.

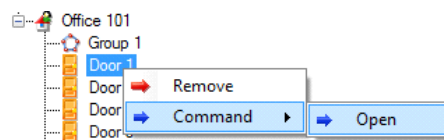


Figure 7-10 Issuing a command to a device

These commands are available for the given devices in both the *Devices* tree and the *Regions* tree. The event information is recorded into the event list of the respective device and into the event list of the given region - for the *Events* tab [see chapter Alarm propagation](#).

7.2.1 Allowing access in the Regions tree

The Access tab in the region tree provides a different view of a persons' access rights that are managed by the ATS8600 Integrated Security Management System. By using this tab you can view and set up the access rights of individual persons using the *Regions* structure. This provides a better understanding of how devices are grouped together in the system based on their location.

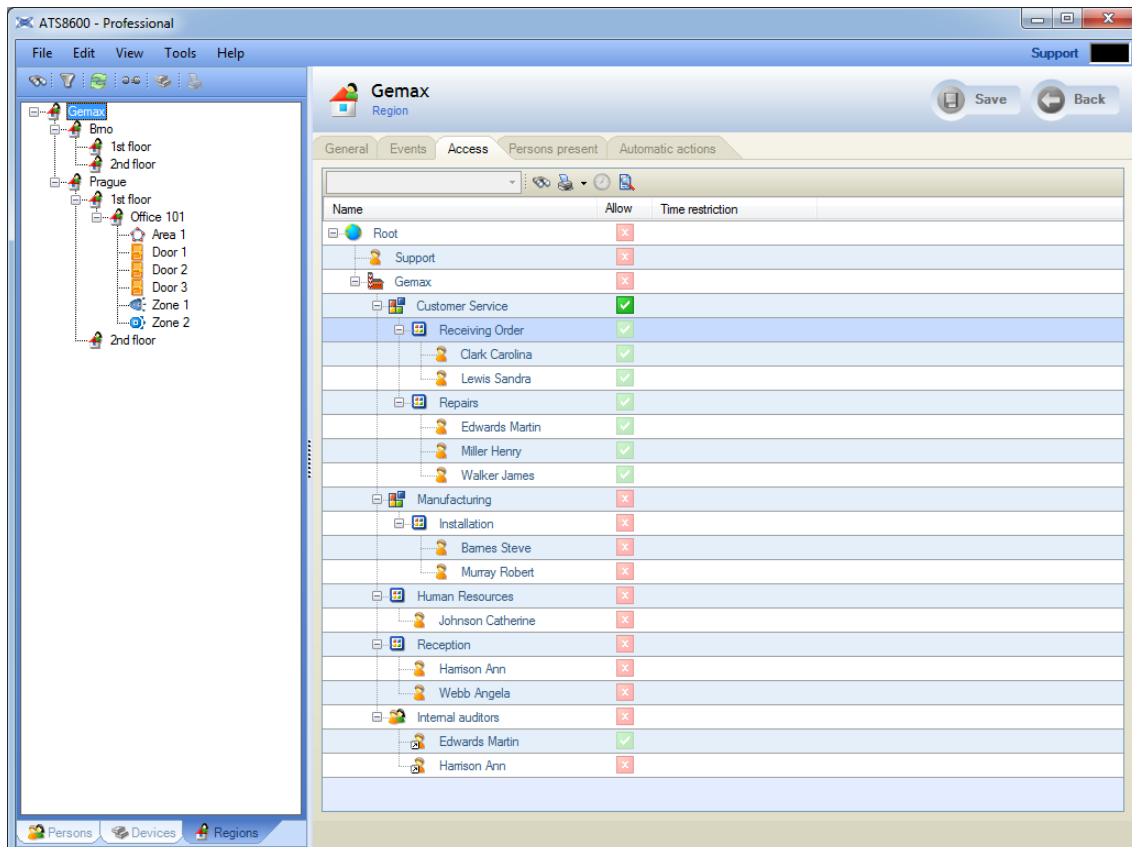


Figure 7-11 Setting the access rights in the Regions tree

A detailed description of how to set up the access rights, including the time restrictions, is provided [in chapter Access rights](#).

7.2.2 Number of persons in the region

It is possible to calculate the number of people present in every region. The calculation is performed on the basis of card usage (employee and visitor cards) when entering and leaving a region. Accordingly, to calculate the number of people present in the region, a card reader must be present to register entry (typically outside of the region) and exit (typically inside a region with the exit door). This setting needs to be applied on the relevant readers by selecting the Reader direction.

Note:

It is a software functionality that can (but does not have to) reflect the device settings for antipassback or other properties.

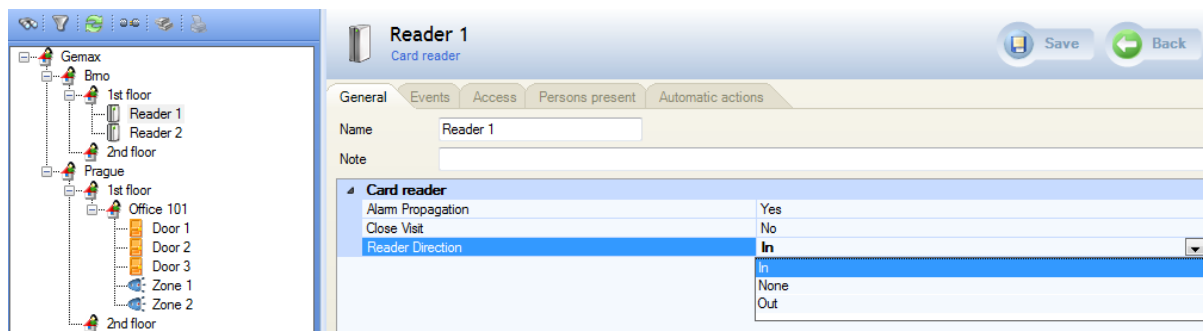


Figure 7-12 Reader direction setup

The next step is to enable person-counting in the given region. Go to the region and in the *General* tab, set *Enabled* to *Yes*.

You also need to set up the *Counting method*. This value determines the persons that would be counted as present in the given region. The default value is *None*. Change it to *Region and all subregions*.

The last configurable value is *Person limit*. If the number of persons present reaches this limit, an event will be recorded about reaching of the person limit and the user can respond to it.

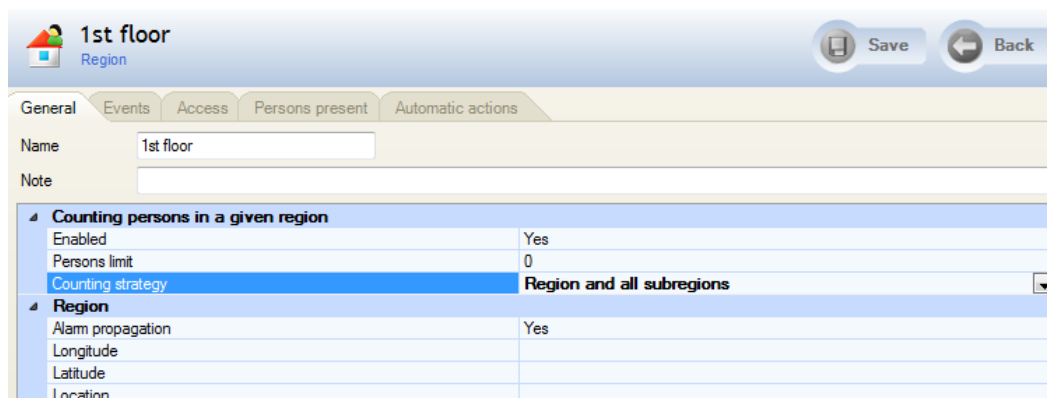


Figure 7-13 Counting setup

The list of the people present in the given region can be viewed in the *Persons present* tab.

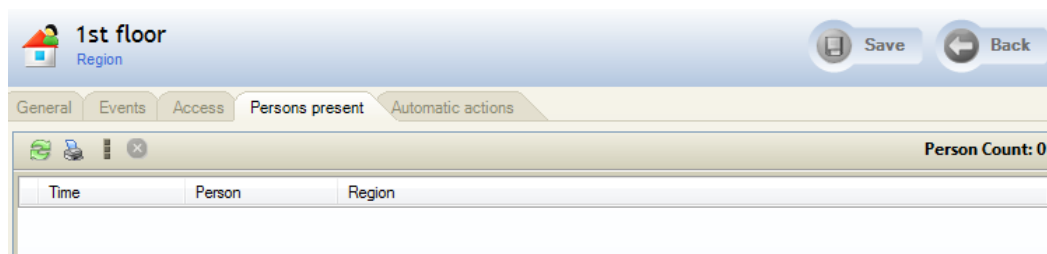


Figure 7-14 Persons present list tab

The list of persons present can also be viewed on the *Monitor* panel when viewing the given region.

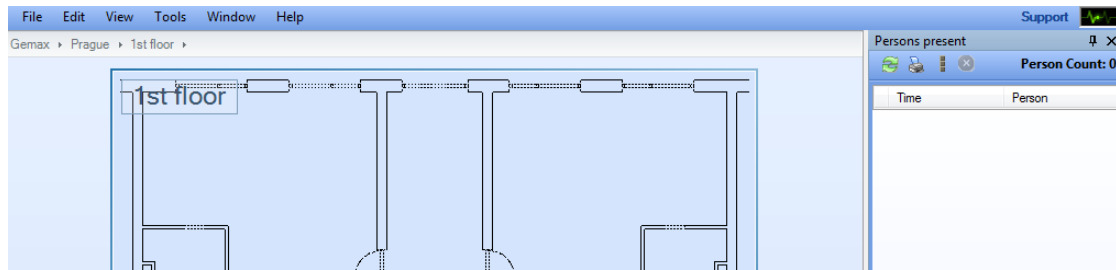


Figure 7-15 Persons present in the Monitor panel

Note:

Starting this function requires a **Reinitialization** of the **Message Broker** node in the **Devices tree**.

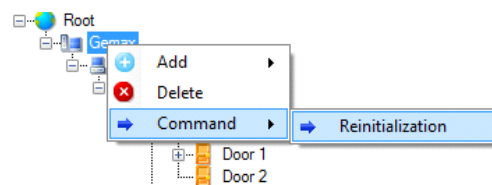


Figure 7-16 Node reinitialization Message Broker

After structural changes in regions or adding readers and keyboards, you need to restart the services of the ATS8600 system in order to ensure their correct functionality. Right-click **My Computer** on the server and select **Manage**. A new window appears. Go to the **Services** tab and restart **Message Broker** and then **Device Manager**. Do this by right clicking the respective service and select **Restart**.

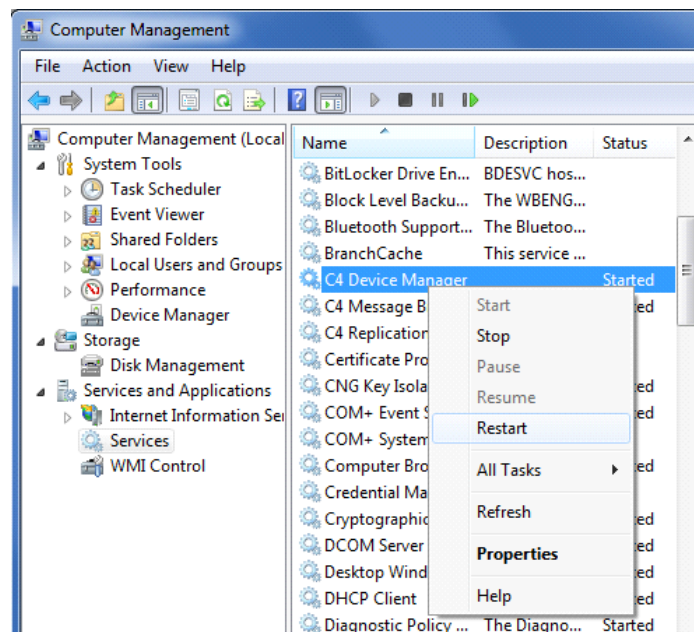


Figure 7-17 Restarting the Device Manager

8 Assets

An *Assets* in ATS8600 represents the Facility Management panel. It serves for administration activities related to the technical documentation of all objects in the system (devices, regions, etc.). It ensures the register of installations, devices replacements, inspections and contact data about service centres.

To open an *Assets*, select *Assets* from the *Tools* menu.

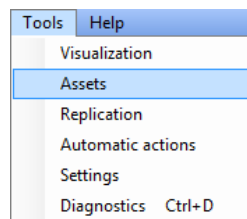


Figure 8-1 Selecting an *Assets*

The *Assets* window consists of a logical tree on the left, which includes a hierarchical structure of regions and devices.

By clicking the required region or devices, a list of technical information about that object (*Assets*) appears on the right.

The *Assets* has a modular structure and is customisable according to the customer's requirements. The following images are only examples (demos).

The customer can define, according to their individual needs, an exact list of items that they wish to register for a particular object. For the given type of the object, a concrete list of items that should be registered for the object can be set.

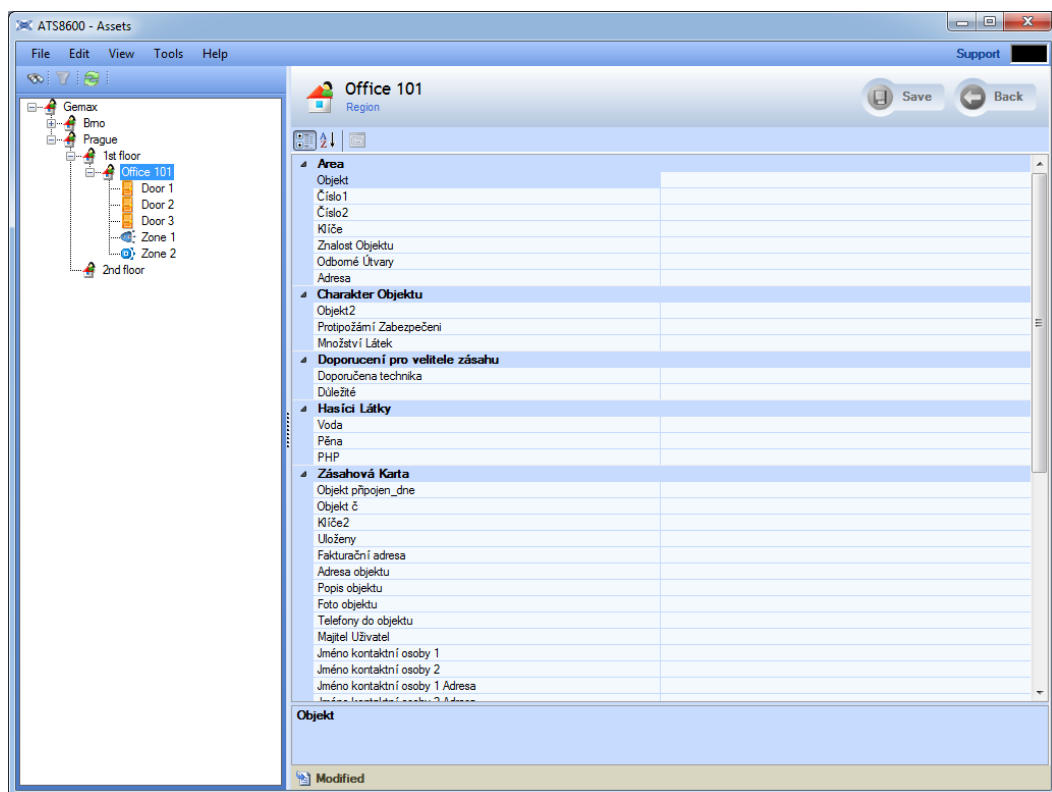


Figure 8-2 Displaying an Assets

The print form of the Assets is accessible by clicking the *File* menu, option *Print - Assets*.

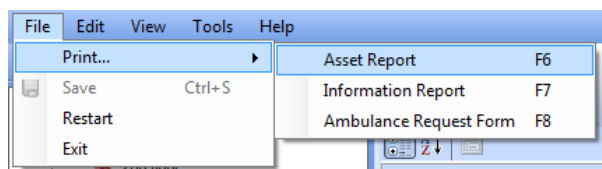


Figure 8-3 Printing an Assets

This function will open the Assets form, where the registered information is displayed in a structured form.

This form is created according to individual requirements of the customer. The figure below contains a demo of the Assets. A concrete form type for printing the object can be set for the given type of object.

Objekt:		OPERATIVNÍ KARTA
KLÍČE:	ZNALOST OBJEKTU:	ODBORNÉ ÚTVARY:
ADRESA (trasa):		

CHARAKTER OBJEKTU

Objekt:
Protipožární zabezpečení:
Množství látek:

HASÍCI LÁTKY

Voda -
Pěna -
PHP -

DOPORUČENÍ PRO VELITELE ZÁSAHU

Doporučená technika
Důležitost :

Figure 8-4 Example of a printed Assets

The *Information card* function provides a different view on the *Assets*. To run this function, select *Print - Information card* from the *File* menu. Here you can place a form to be used when setting up an event. This function is also customisable according to customer's needs. Figure below shows an example in which an information card can be, for instance, an *Intervention Log*. For the given type of object, a concrete type of the information card can be set.

Objekt připojen dne:	Objekt č.:
Důvěrné informace tvoří obchodní tajemství. Nesmí být poskytnuty třetí osobě!!	
ZÁSAHOVÁ KARTA OTROKOVICE	
Klíče:	
Uloženy:	
NÁZEV OBJEKTU:	
Fakturační adresa:	
ADRESA OBJEKTU:	
POPIS OBJEKTU:	FOTO:
Telefony do objektu:	
Majitel / uživatel /:	
Jmeno kontaktní osoby:	Adresa
Telefon	Mobil
SPECIÁLNÍ SMLUVNÍ DOHODY:	
Servis provádí firma:	Telefony:
Převod. tabulka:	Ústředna:
Vysílač:	
POŽÁRNÍ SIGNALIZACE:	VOLAT HASIČE:
Počet čidel:	Telefon:
TÍSŇOVÁ SIGNALIZACE:	
Specifikace a umístění:	
Způsob přenosu signalu:	Telefon:

Figure 8-5 Example of an Information card

Predefined information registered in the *Assets* is also displayed in the *Monitor* panel when the incident of the given object occurs. This function contributes to the prompt delivery of an important piece of information to the person responsible.

Note:

For your specific requirements for the customisation of the system regarding the *Assets*, please contact your supplier.

8.1 Automatic reports print set-up

Asset reports can be printed automatically.

In case of an alarm, a message is automatically sent to a predefined client PC printer and is also printed out.

To activate this function, you need to give the user the Automatic Report Printing permission in the *Persons* tab. *Alarm management* must also be active in *System settings*. ([see chapter Overall enabling or disabling of Alarm management](#))

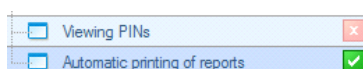


Figure 8-6 Permission to automatically print reports

9 Replications

The ATS8600 system includes a connector to external information systems (IS). This connector provides interconnection between ATS8600 and another information system, most commonly a HR system of the company.

The practical use of replication is that it eliminates the duplicate registration of data: in the HR system and the ATS8600 Integrated Security Management System.

Replication makes it possible to import data from the personnel system to ATS8600. The ATS8600 import tool (*Replication Manager*) can customise its interface to connect with other IS (e.g. SAP, Odyssea).

To open the *Replications* panel, click *Replications* in the *Tools* menu.

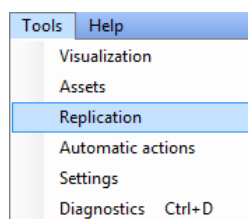


Figure 9-1 Panel selection Replications

If no connector to another IS is established into ATS8600, the *Replications* panel is empty. In order for the *Replication Manager* to function correctly, the MAC address must be entered in the *Address* box in the *Root* node.

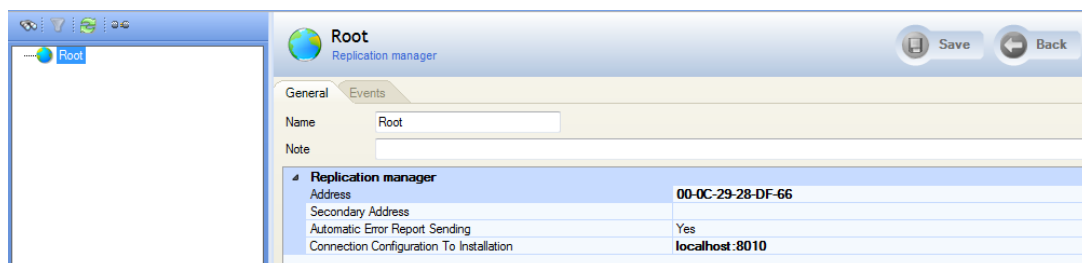


Figure 9-2 Replications window

9.1 Connector to external IS

First it is necessary to add a connector to the IS from which you wish to import the data. Right-click *Root* and select *Add - Personnel system* from the pop-up menu.

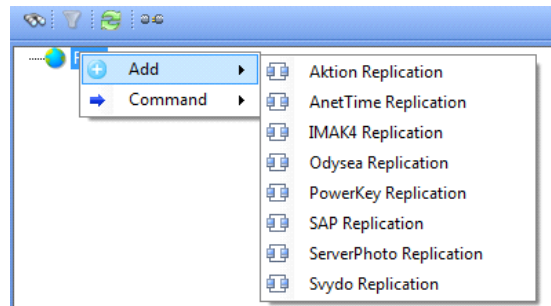


Figure 9-3 Creating a connector to another IS

Enter the connector's attributes in the right-side window:

- **Name:** Connector description.
- **Enabled:** True to enable the use of this connector
- **Connection:** Connection string to external database of the IS conform MS standards.
- **Account:** IS database username (SQL username in case of SQL authentication).
- **Password:** IS database password (SQL password in case of SQL authentication).

Odyssea Connection	
Name	Odyssea Connection
Note	
Circuit	
Enabled	Yes
Odyssea Replication	
Connection	Data Source=localhost;Initial Catalog=DbName;Integrated Security=SSPI;
Account	
Password	
Command execution timeout	30
Procedure	
Primary key	External Number
Managed organization unit	

Figure 9-4 Connector attributes

To initialise the connector, click **Run**. Running the connector means that it will be available for performing a replication of required data.

Performing **Stop** will hold the replication to the connector, until it is started again or the *Replication Manager* is started.

By using **Reinitialization**, the connector is re-started with the latest configuration.

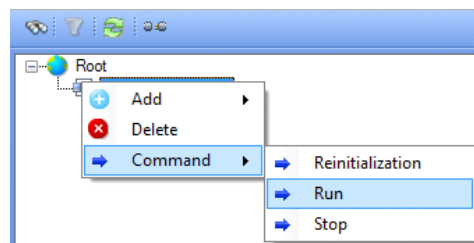


Figure 9-5 Connector functions

9.2 Replication settings

Next it is necessary to set the tasks for performing data synchronisation. Right-click the connector and select *Person replication* from the pop-up menu.



Figure 9-6 Creating a task for data synchronisation

Enter the name for this task and set its parameters.

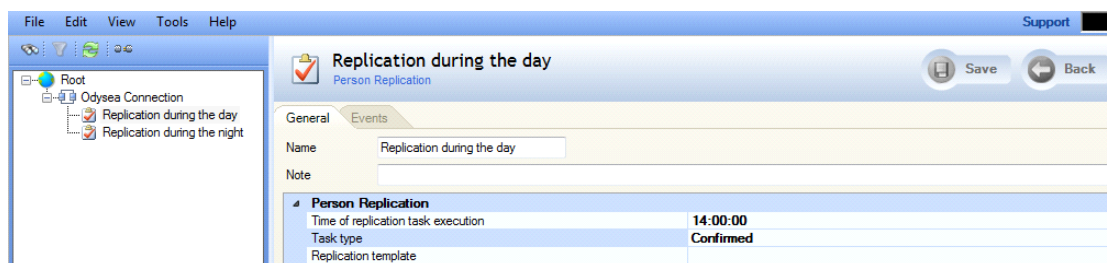


Figure 9-7 Creating a task for data synchronisation

For each task the following parameters are required:

1. Time of replication task execution - setting the time for importing the changes from the HR IS to ATS8600.
2. Task type
 - automatic
 - semi-automatic (confirmed replication)

When selecting the replication type it is necessary to determine who is responsible for the accuracy of the ATS8600 data.

Automatic replication is used when an HR member is responsible for correctness of the data in the personnel system as well as in ATS8600. It means that all newly registered data and changes will be automatically reflected into ATS8600 at specified regular intervals (usually at night).

It is advisable to set the time of the automatic replication task for before midnight so that the changes are reflected in the scheduled sending of credentials to devices.

Semi-automatic (confirmed) replication is used when the person responsible for the data in ATS8600 is someone other than an HR member responsible for the data in the personnel system. With this type of replication, the data import into ATS8600 will take place at the set time, but updating (overwriting) the data must be confirmed by the responsible person. It means that the list of names to be imported is waiting in the "buffer stock" to be confirmed. Only upon confirmation will the data be synchronised with ATS8600.

A created task can be deleted or you can issue a command for replication immediately (in addition to the set time). To run the import of modified data into ATS8600 immediately, click **Replicate**.

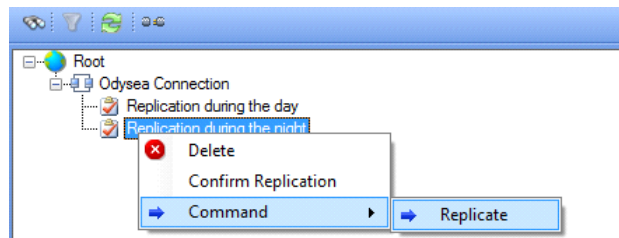


Figure 9-8 Task functions

Using the automatic action, it is possible to send the responsible person an email notification about the import ([see chapter Automatic actions](#)). To set up email notifications, Replication events must be turned on. Define the person responsible for confirming the replication in the automation settings.

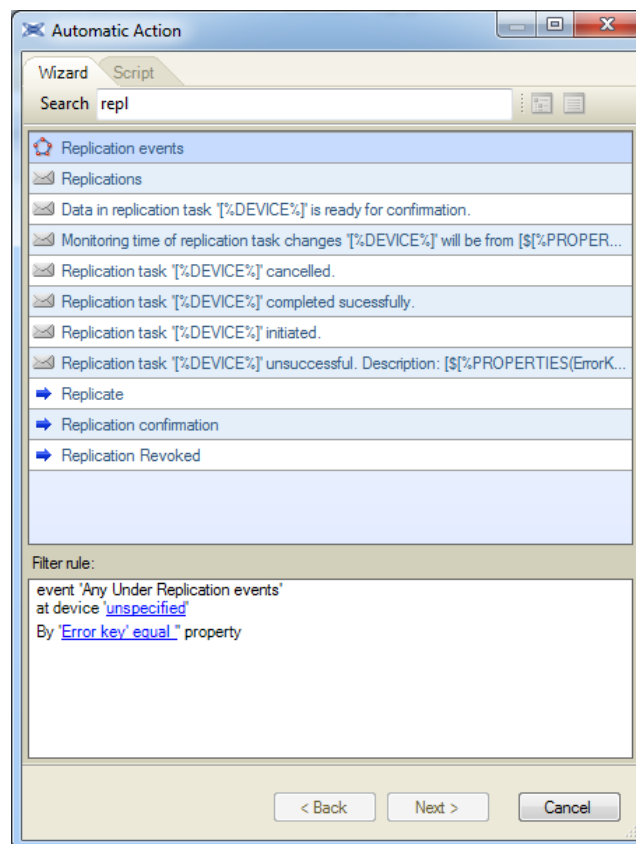


Figure 9-9 Setting an automatic action

Note:

Changes in the configuration of the connector or tasks will not take effect until you restart the connector by clicking **Stop** and then clicking **Run**.

9.2.1 Confirming the replication

The responsible person confirms the replication by right-clicking the task and selecting **Confirm replication** from the pop-up menu.

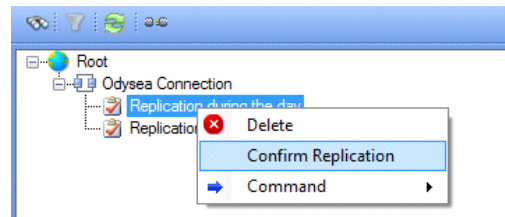


Figure 9-10 Confirming a replication

During the confirmation itself, the responsible person sees the complete and detailed list of changes to be performed: newly registered data, modified data, transfer of persons in OS etc.

Supported synchronisation operations

- *Creating a person*
 - if a person is added to the HR IS that not yet existed in ATS8600. This operation includes assigning the person to the organisational structure.
- *Modifying a person*
 - the person exists in both systems, but some data has changed.
- *Modifying the assigning of a person*
 - person already exists in both systems, but the pairing has changed.
- *Denying a person*
 - the registered status of the person in the HR IS has changed from Granted to Denied. In ATS8600 the person will be set to "Blocked" status (unable to log in to ATS8600 and prevented from being send to devices).
- *Allowing a person*
 - reverse operation to denying a person.
- *Deleting a person*
 - the person will be deleted from ATS8600 Integrated Security Management System.
- *Creating a credential*
 - the card was imported from an HR IS. It will be created in ATS8600.
- *Modifying a credential*
 - after import, some attributes of the card have been changed (e.g., name, status, owner, administrator).
- *Deleting a credential*
 - credential is no longer a part of the HR IS, so it will be deleted from ATS8600.

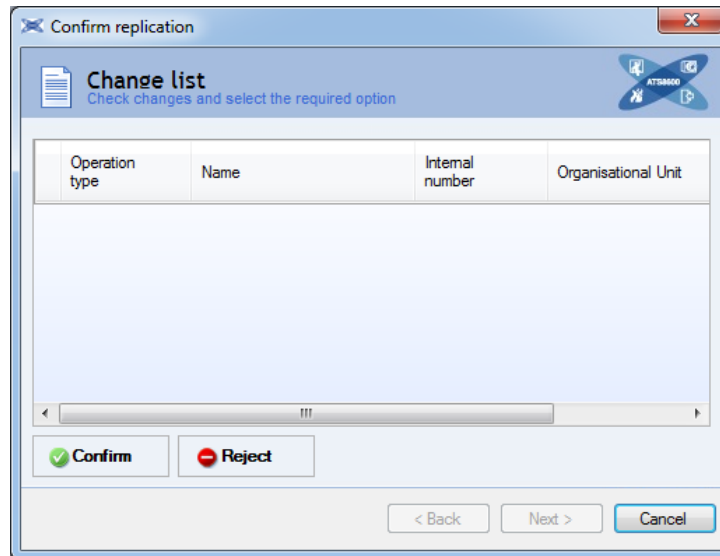


Figure 9-11 List of names for confirmation

During the replication confirmation, the responsible person will assess each change individually. If you agree with the change, select it and click the **Confirm** button. Upon confirming, the changes will be applied to the ATS8600 database.

If you want to reject a change to ATS8600, click **Reject**.

9.2.2 Event monitoring

Each connector to another IS as well as each replication event is listed in the *Events* tab.

For a detailed description of the ATS8600 events monitoring system, [see the chapter Events](#).

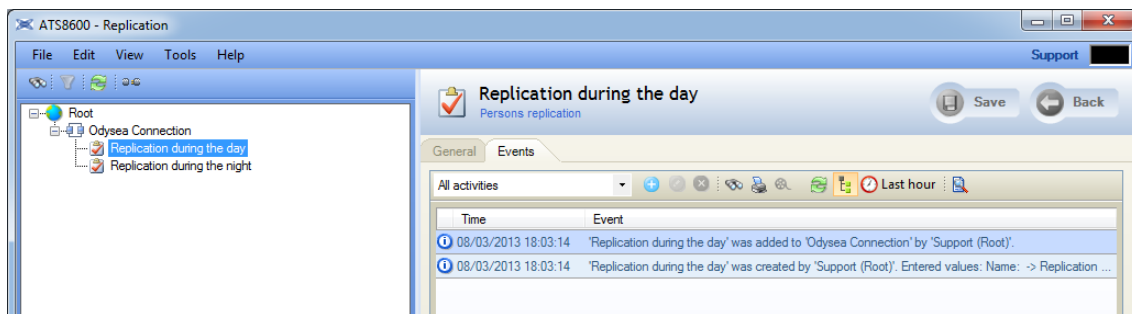


Figure 9-12 Event monitoring

Warning:

Before running a replication job, it is necessary to run the ATS8600 Replication Manager service, which is set for manual starting by default. If you plan to use replication for a longer term, enable the service to start automatically (Services - Startup Type - Automatic).

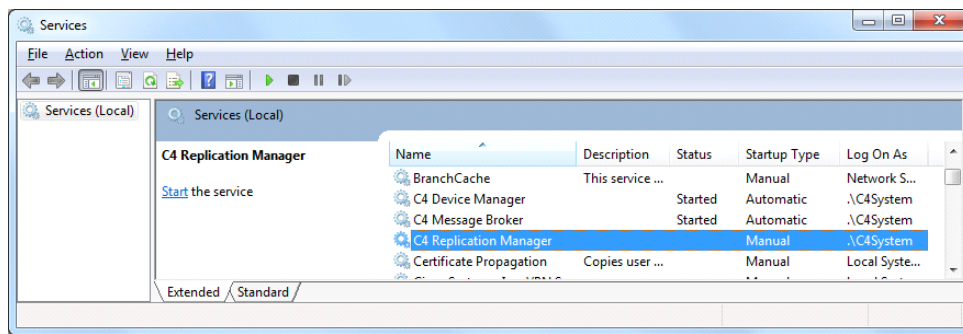


Figure 9-13 ATS8600 Replication Manager service

10 Visualization

Visualization offers a method to show the location of devices or groups of devices on maps using the region structure. It provides a quick view to dispatchers about the status of the system and the location of issues.

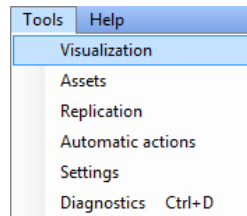


Figure 10-1 Visualization option

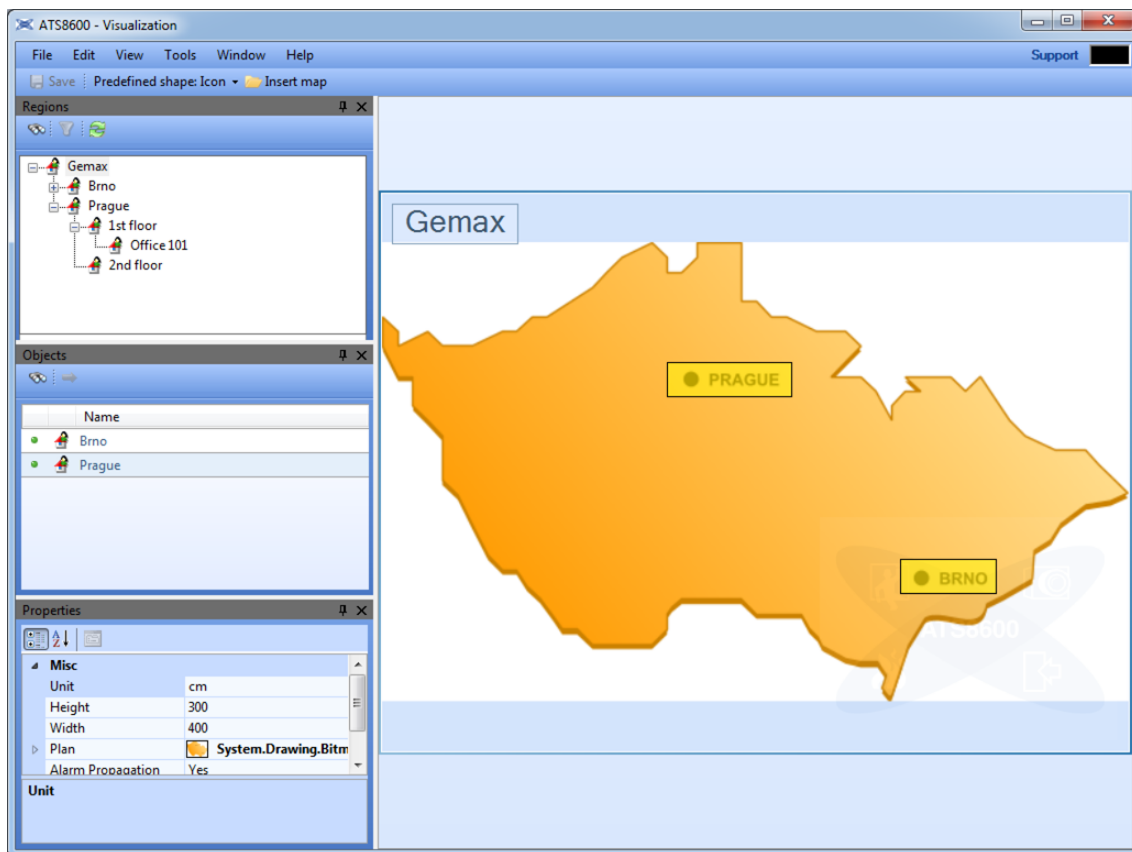


Figure 10-2 Visualization panel

The *Visualization* panel screen consists of the visualization panel and auxiliary windows:

- *Regions* - shows the hierarchical structures of regions and subregions
- *Objects* - this window shows objects of the region selected in the *Regions* window
- *Properties* - summary of properties of the selected region or object.
- *Devices* - hierarchical device structure is displayed.

The placement and display of these windows on the visualization panel screen can be customized. To open a window, click in the *Window* menu. Click again to will close the window.

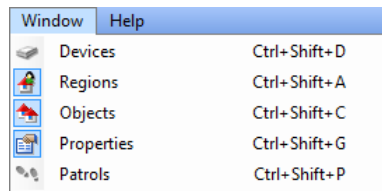


Figure 10-3 Window menu

Each window can be moved to any part of the screen using drag & drop. The arrow icon displayed when dragging a window and indicates a window placement in the full-screen environment in the direction of that arrow. If you want the window to adjust to the whole screen, drag the windows over this icon and release. This system of window placement is also used in the *Monitor* and *Cash desk* monitor panels (see chapter Events and [Cash Desk Monitor](#)). On each window you can also turn on the auto-hide function (pin).

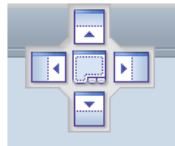


Figure 10-4 Indication of window placement

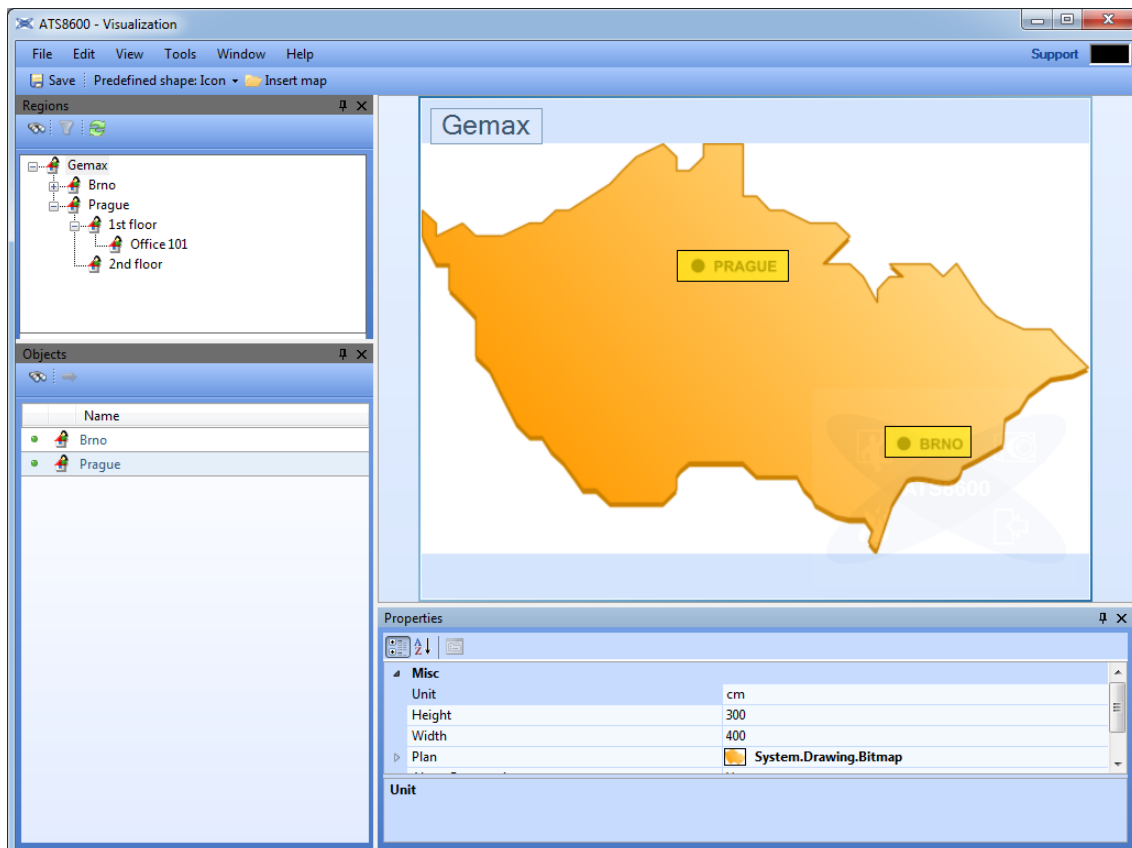


Figure 10-5 Change of window position

10.1 Example of visualisation

Every region can be graphically represented either by its picture or its ground plan.

When creating a visualisation is it important to:

- start from the top structure when using the region structure and work your way through to the subregions;
- create links between the individual levels of regions and subregions.

The example lists the visualisation procedure of the Gemax company.

1. The *Regions* window of the visualisation panel shows the hierarchical structure of regions as created in the *Regions* tree.

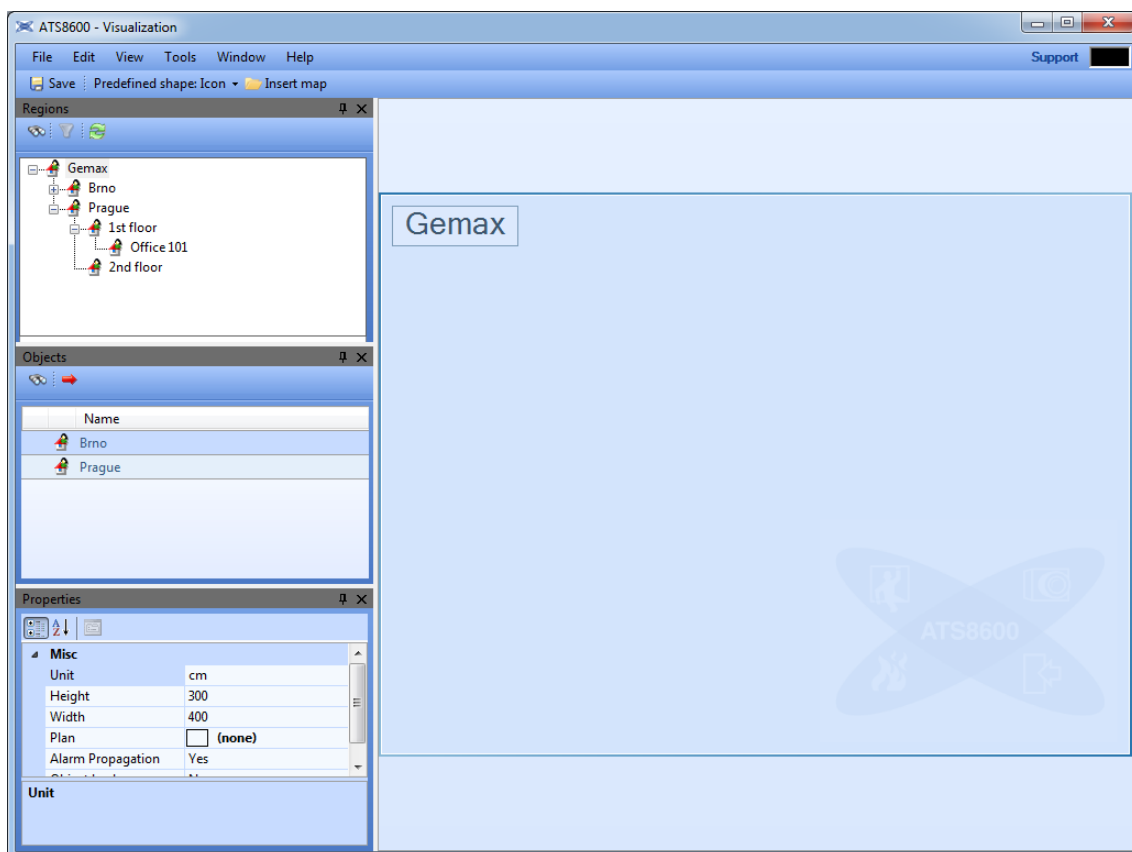
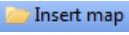


Figure 10-6 Visualization of Gemax

2. Select the highest level of the region (Gemax) and click . The computer folder structure appears, from which the file containing the region map is selected. This map is added to the visualization panel as a background on which devices and other elements are placed. Supported formats for maps: *.jpg, *.jpeg, *.bmp, *.png, *.wmf, *.emf, *.gif. The maximum recommended size of the ground plan file is 6 megapixels with 4:3 aspect ratio.

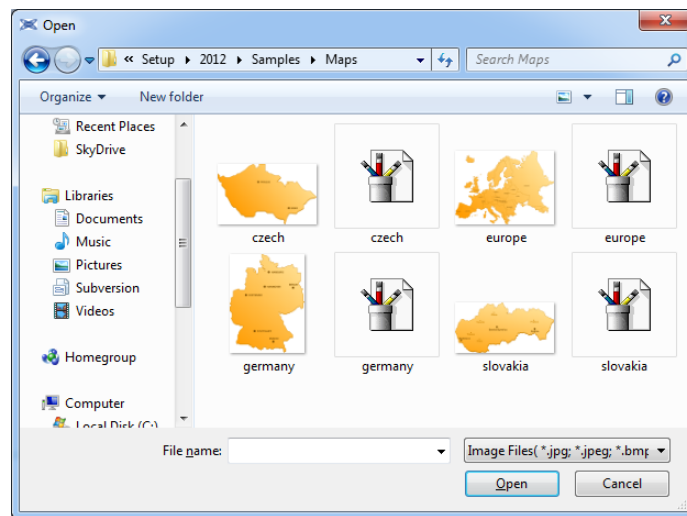


Figure 10-7 Inserting a ground plan from a PC disk

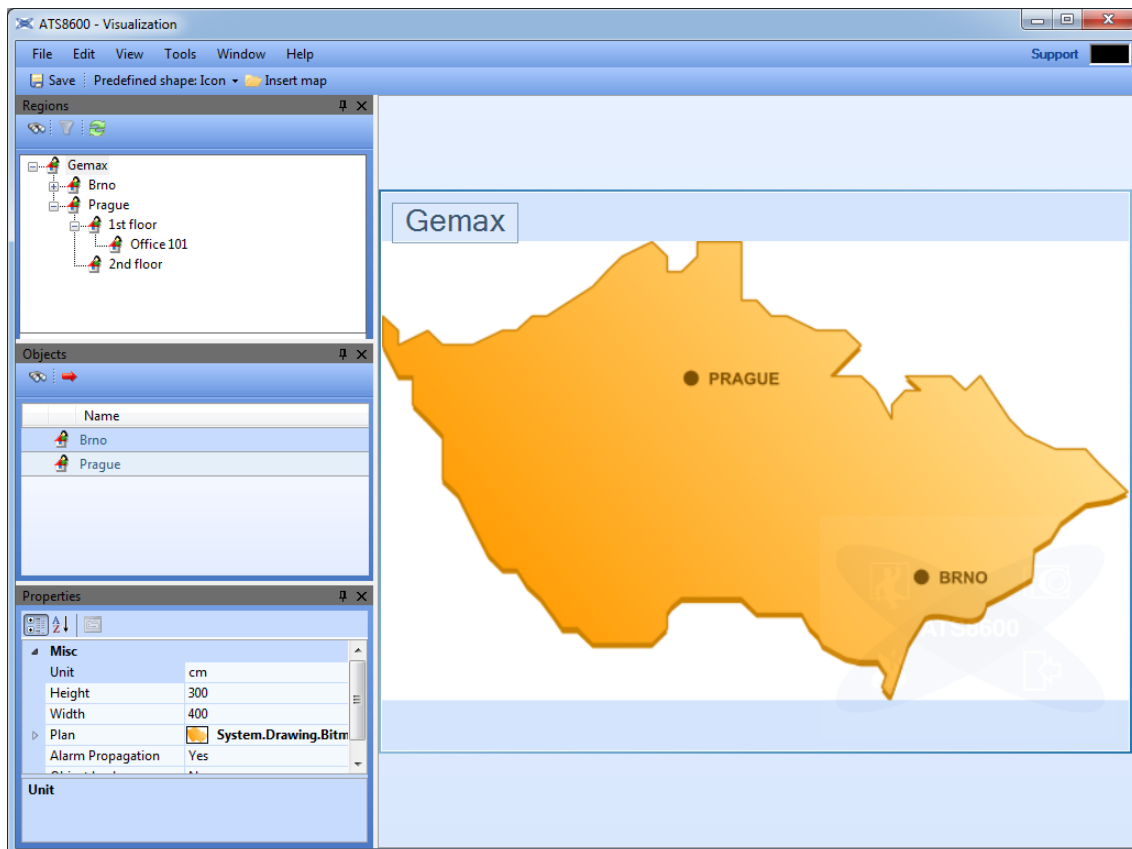


Figure 10-8 Inserted map

3. Now you have to locate all branch offices of Gemax on the map of the Czech Republic: Prague and Brno. To select a branch on the map, draw a rectangle. In the upper toolbar, select **Predefined shape: Rectangle** Predefined shape: Rectangle ▾.
4. From the *Objects* window, drag objects Prague and Brno and drop them to the respective locations on the map.

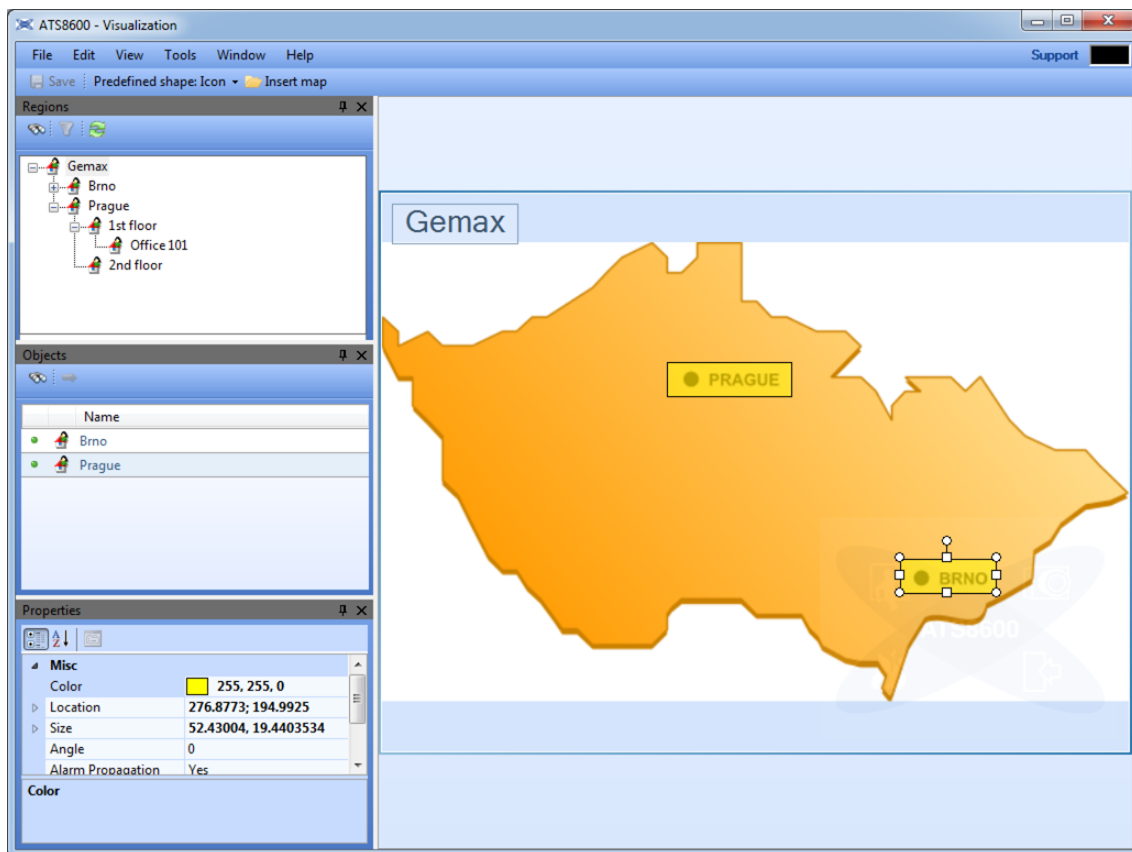


Figure 10-9 Visualization of branches

5. Select the Prague sub-region in the *Regions* window and click [Insert map](#) to browse the PC disk for the ground plan of the Prague branch. Insert the ground plan for the Brno branch in a similar way.

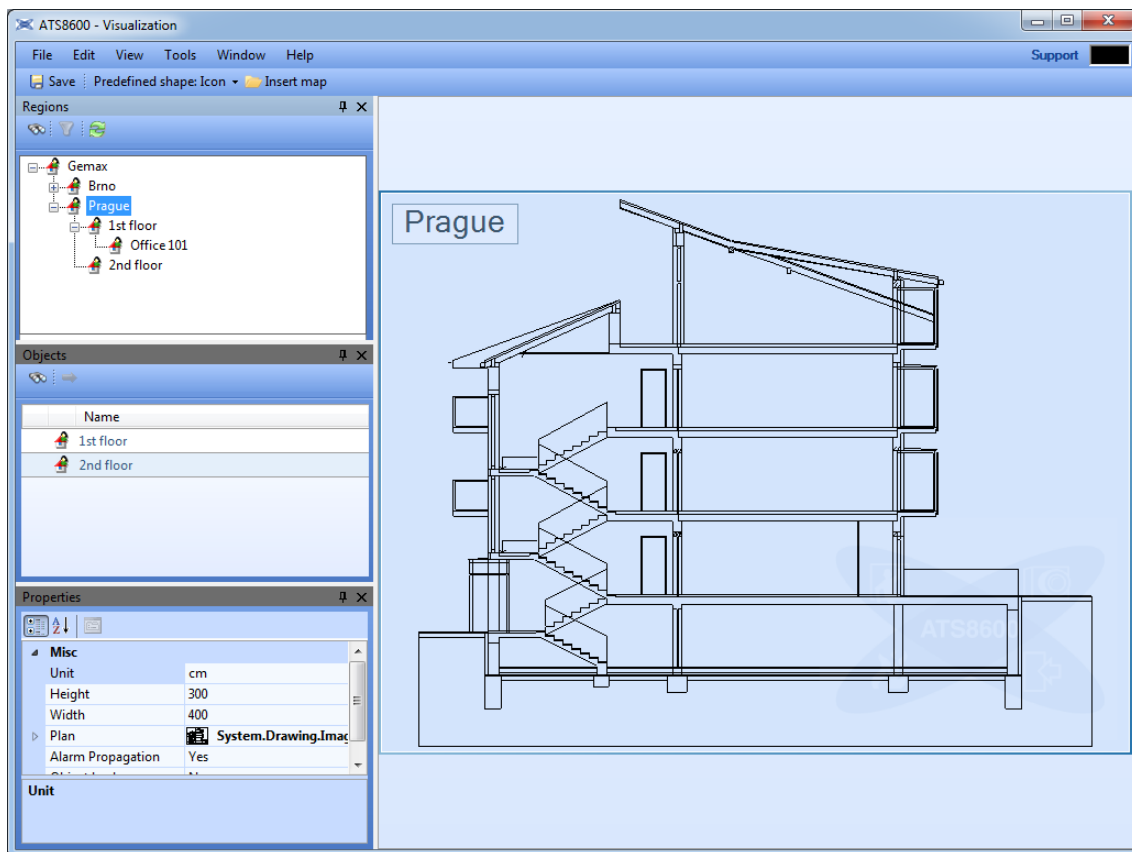


Figure 10-10 Inserted map of the Prague branch

6. Now we will visualize floors on the Prague branch ground plan. To select a floor, draw a rectangle. In the upper toolbar, select **Predefined shape: Polygon** Predefined shape: Polygon ▾.
7. From the *Objects* window drag objects 1. Floor and 2. Floor and drop them to the respective spot on the ground plan.

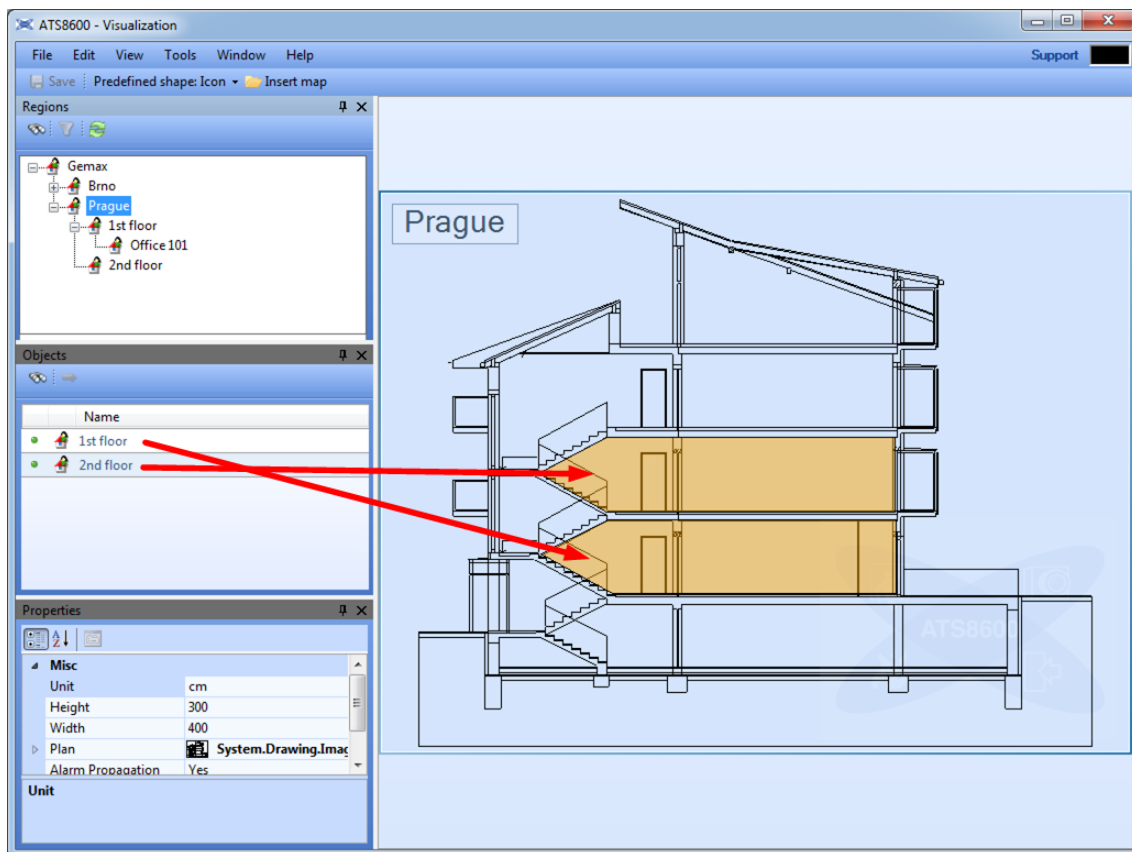


Figure 10-11 Visualization of floors in the Prague branch

8. Select the 1st Floor visualized sub-region in the *Regions* window and click  **Insert map** to browse the PC disk for the ground plan of the first floor. Insert the ground plan for the second floor in a similar way.

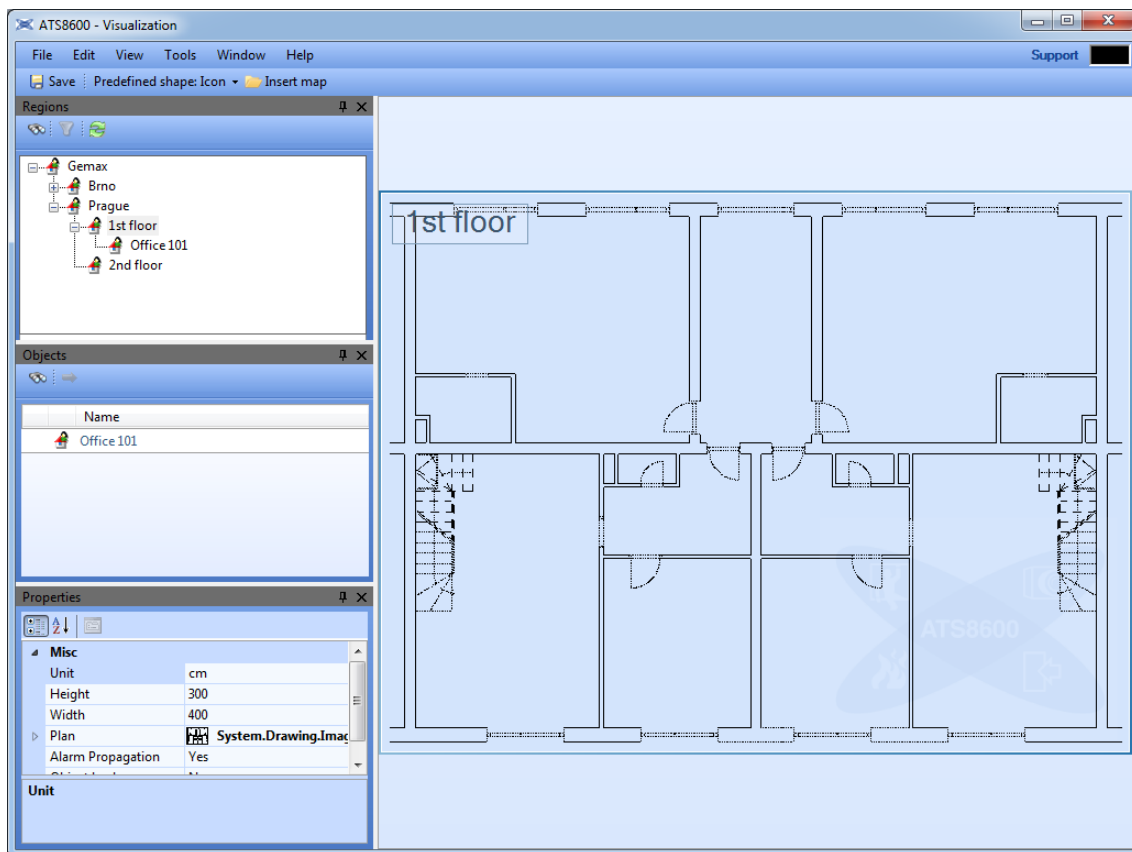


Figure 10-12 Inserted map of the first floor

9. Now we will visualize the office in the first floor of the Prague branch ground plan. To select an office, draw a rectangle. In the upper toolbar, select **Predefined shape: Rectangle**
Predefined shape: Rectangle .
10. Drag and drop the Office 101 object from the *Objects* window to its respective location on the ground plan.

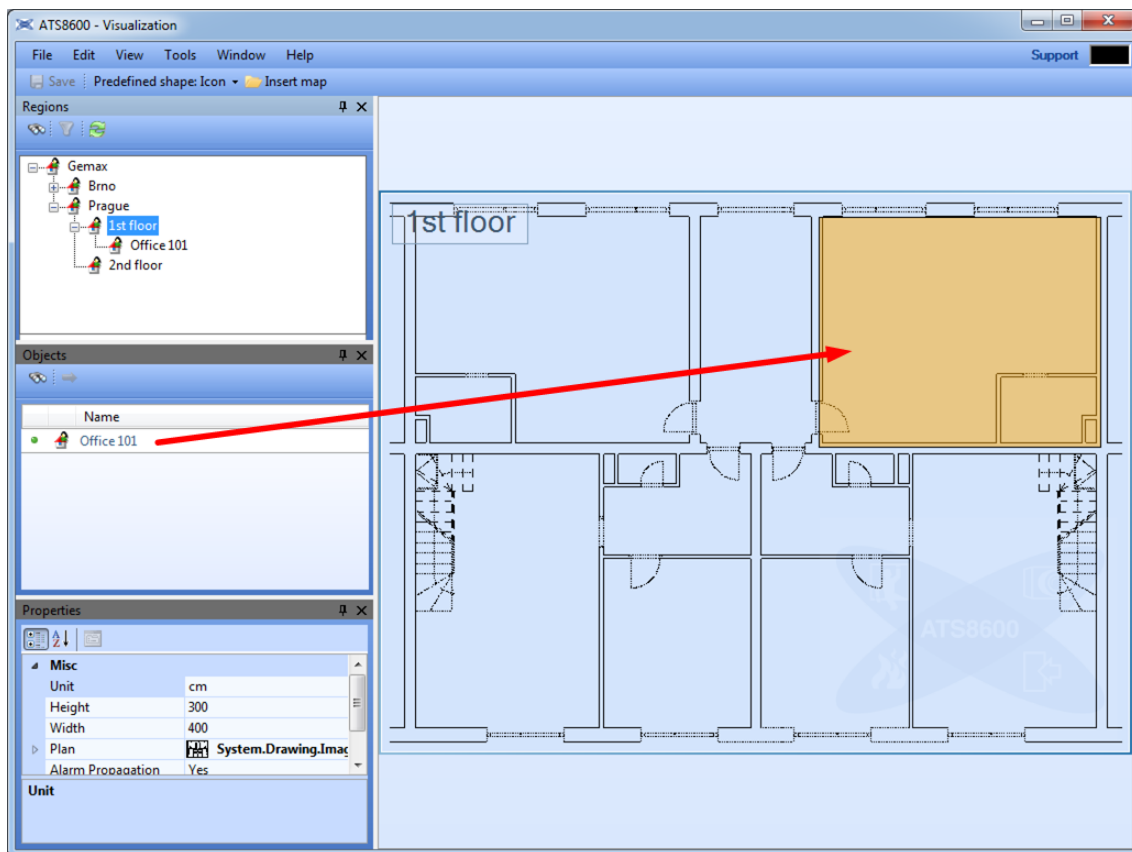


Figure 10-13 Visualization of an office on the first floor

11. By marking the Office 101 object, a devices list with all devices present in the office appears in the *Objects* window
12. Use the ground plan of Office 101 for device placement.
13. To select a device on the ground plan, place an icon. In the upper toolbar, select **Predefined shape: Icon**.
14. From the *Objects* or *Devices* window, drag a device and drop it to the respective spot on the ground plan.

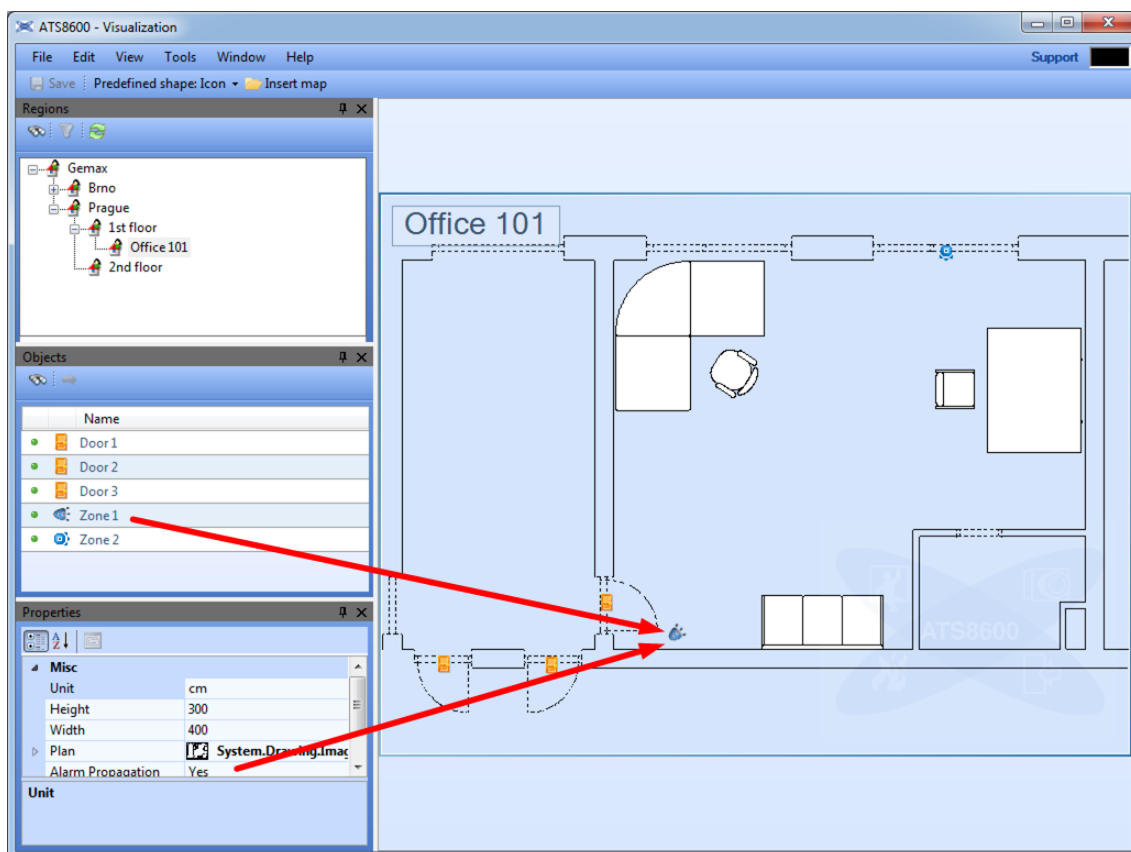


Figure 10-14 Placing a device on the map

15. Click Save.

Note:

The object that is visualised on the ground plan is marked with a ball in the *Objects* window. This distinguishes between visualized and non-visualized objects.

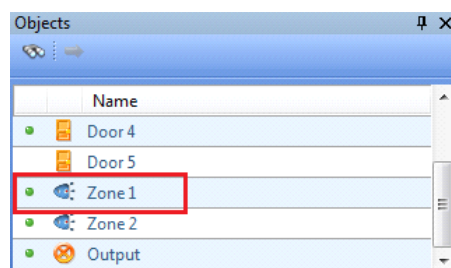


Figure 10-15 Marking a visualized object

10.2 Auxiliary windows description

10.2.1 Regions

- Displays the *Regions* tree. The content of the *Regions* tree must at first be created in the *Professional* panel.
- This window is used for selecting the region whose content would then be displayed on the visualization panel.

10.2.2 Objects window

- Contains objects in the selected region that can be visualized on the map. These objects can be divided into two categories.
 - sub-regions of the selected region,
 - devices placed into the region.
- Items of this window can be dragged by a mouse and dropped over the panel, which creates a visualization element. Items that are displayed on the panel are marked with a green dot, located next to their item names.
- Items can be removed by selecting the item and clicking **Remove** button (). Removing an item removes it from the panel, as well as the *Objects* window. The effect of removing an item with respect to the rest of the application depends on the item's category:
 - sub-regions are removed from Visualization and the *Regions* tree,
 - devices are removed only from Visualization, but not from *Devices* tree.

10.2.3 Devices window

- Displays the *Devices* tree. The content of the *Devices* tree must be created first in the *Professional* panel.
- Items of this window can be dragged by a mouse and dropped over the panel, which
 - creates a visualization element and
 - an item in the *Objects* window.

This speeds up the process of adding devices to the visualization panel.

Another way to do this is by adding the device into the *Objects* window list ([see chapter Device structure in a region](#)) and subsequently adding it to the panel.

The *Devices* window saves time that would otherwise have to be spent

- by addition of the device into the *Objects* window and then to the *Visualization* panel,
- by constant switching between the *Professional* and *Visualization* panels,
- and by selecting a region after switching to *Visualization*.

10.2.4 Properties window

It contains customizable parameters of the currently selected item, or the visualization panel. The descriptions of available parameters can be found in [in chapter Properties of visualisation elements](#).

10.2.5 Patrols window

It displays a patrol tour list and allows patrol modification. Patrol functionality is described in detail [in chapter Patrol tours](#).

10.3 Properties of visualisation elements

You can use various predefined shapes in the graphical representation of individual regions, subregions and devices. They are graphical items, which help to localise the subregion from higher levels.

The predefined shapes are thus elements that are used in region and device visualisation. Click **Predefined shape: Icon** to set the predefined shape you wish to use in the visualization:

- Icon - for visualisation of devices
- Rectangle - for visualisation of regions or areas
- Ellipse - for visualisation of oval regions or areas
- Polygon - for visualisation of polygonal regions or areas
- Multidetector - special type for perimeter systems. It is not recommended to use it for other types of visualisation.
- Button - visualization of a button with assigned automatic action.
- Laser detector - special type for laser motion detectors; not recommended in other types of visualisation
- Label - special type for Label element (a custom description) visualisation created in the *Regions* tree. The Label shape does not support status display. If you visualize a device as Label, the device name appears on the ground plan. The text color on the *Monitor* panel will be static according to the set shape properties.

All the shapes mentioned can be graphically adjusted. Select the element in the visualizer to be able to use the mouse to

- rotated (e.g., rotation of the camera icon )
- moved

You can change the size of the element; however, devices are differentiated by the shape of the given element

- all elements except for the Icon can be increased/decreased in size with a mouse
- the size of the Icon can be chosen in the Properties window. There are three options:
 - a) Small,
 - b) Medium,
 - c) Large.

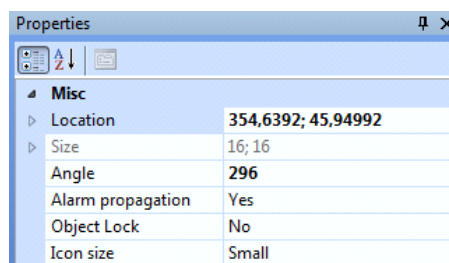


Figure 10-16 Icon properties

Icon sizes are important in case of an alarm. If an icon-shaped element activates an alarm, its size on the *Monitor* panel increases by one level.

Right-click to see a menu with functions related to the selected element:

- **Delete** - delete the selected item or map. Deleting an item from the panel does not delete the element from the *Objects* window.
- **Send to back, Bring to front** - Display the the item in front or behind other objects.
- **Lock** - Lock the item to prevent moving on the map.

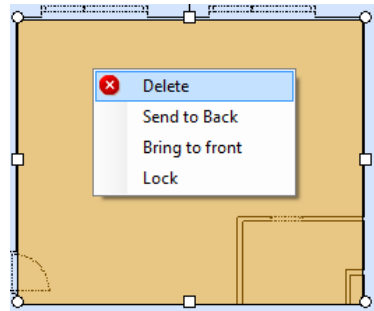


Figure 10-17 Right-click pop-up menu

After selecting an element, the *Properties* window displays properties and the size of the element representing a subregion. These parameters can be set adjusted to suit any graphics.

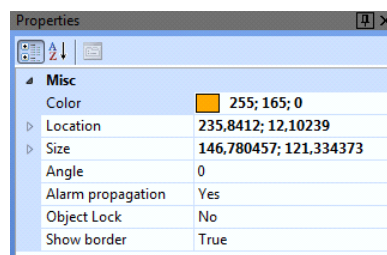


Figure 10-18 Properties of a predefined shape

Click the Color box at the end of this line to see the option to open a color menu for element fill.

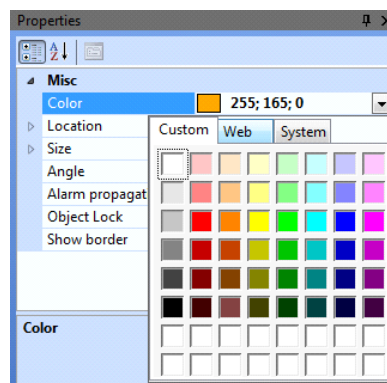


Figure 10-19 Color list for predefined shapes

Other optional parameters of objects:

1. *Alarm propagation* - it is possible to turn off alarm propagation on the object if it should not be propagated to parent regions.
2. *Object lock* - locking the object (setting the value to "yes") secures the object so that it cannot be moved on the map.
3. *Show border* - the set value determines whether the visualisation element will have a

border. The border should be turned off when you do not wish the map to act as a boundary or wall.

10.4 Alarm propagation

Alarm propagation provides the functionality to expose alarms to dispatchers via individual regions and subregions to the object that notifies the alarm. Alarm propagation takes care an alarm in a device is routed to it's parent (e.g. from intrusion zone to intrusion panel). Notification is available in the *Monitor* panel.

Visualisations of alarms is provided through maps showing locations or through devices showing the devices available

So there are two views for each device:

- from point of view of the device (cameras, inputs, zone, etc.)
- from the point of view of the geographical location within the region using maps

In this case, when an alarm occurs the alarm propagation in the *Monitor* would navigate the dispatcher along two separate paths.

To turn off the navigation on one chosen path, turn off the *Alarm propagation*. This function can be turned off in any region to ensure that the alarm will not propagate to the next level above.

This way, navigation along one path can be cancelled, while the alarm is still notified to the dispatcher via the second path.

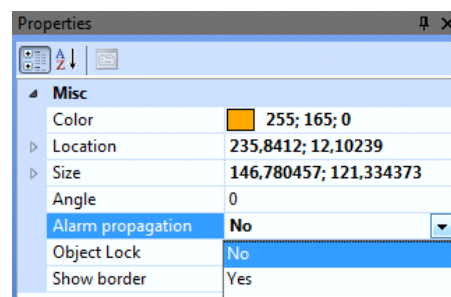


Figure 10-20 Turning off alarm propagation

Example:

Navigation to the incident recorded via a camera will be cancelled in the cameras panel, but navigation to this camera will be maintained via the map of the region.

10.5 Adding a Button in visualization

This chapter contains the procedure for implementing a button and setting up an automatic action that will be performed whenever the button is pressed.

1. Right-click the selected region in the *Regions* tree to create a button that will be displayed in the *Monitor* panel. Else the window will hide automatically if another window becomes active. Enter a button name that describes the action the button performs.

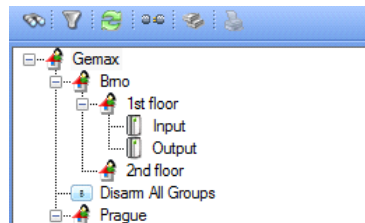


Figure 10-21 Creating a button in the Regions

2. On the *Visualization* panel, select **Predefined shape Button** in visualization Predefined shape: Button ▾ and then drag the *Button* on the map.
3. Click  to start the automatic action wizard.

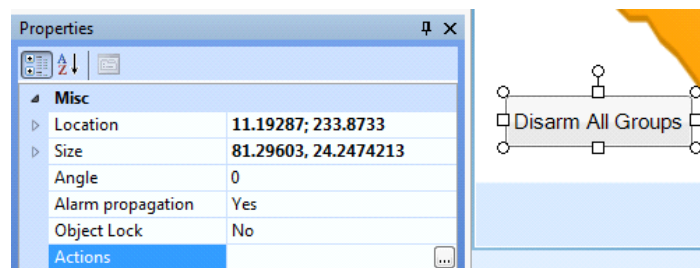


Figure 10-22 Starting the wizard

4. Enter the action that should be performed after clicking the button.

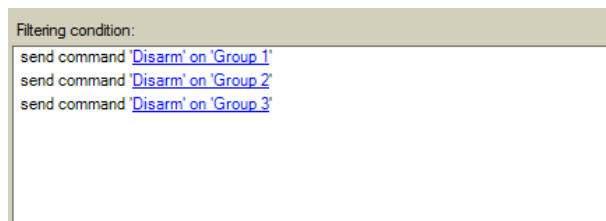


Figure 10-23 Setting up commands that will be performed after clicking the button

5. Enter a descriptive name of the automatic action

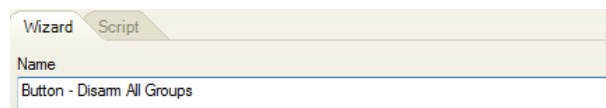


Figure 10-24 Giving name to an automatic action

6. Go to the *Monitor* panel and test the functionality of the created button.

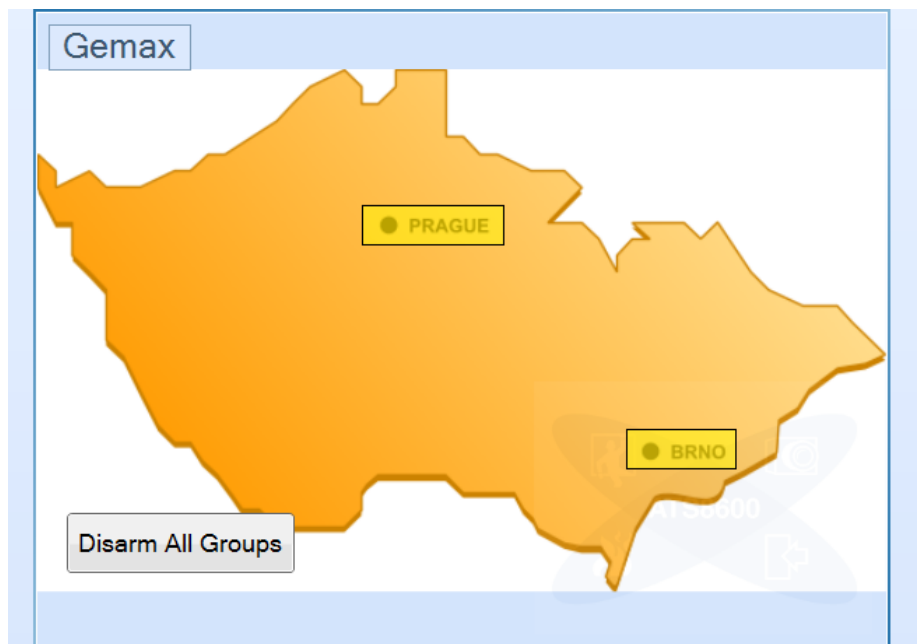


Figure 10-25 Button on the Monitor panel

Note:

In order to be able to use the button in the *Monitor* panel, you need permission for the given region, the given button in the region, and for the **Push** command. A detailed description of the individual types of permissions is provided [in chapter Types of permission](#). The action itself is performed using the permissions of the user who created the action connected with that button. Therefore, it is possible for any user to perform operations that he or she otherwise would not have permission to perform.

Note:

The automatic action can also be modified in the *Automatic actions* panel as well.

10.6 Mask editor

Certain detector types can be visualized using a mask that signals a breach of the guarded area. If the conditions require exclusion of certain areas from guarding (e.g., false alarms caused by the movement of people and vehicles), this change can be performed before using the *Mask editor*.

Clicking  in Visualization launches the *Mask editor*.

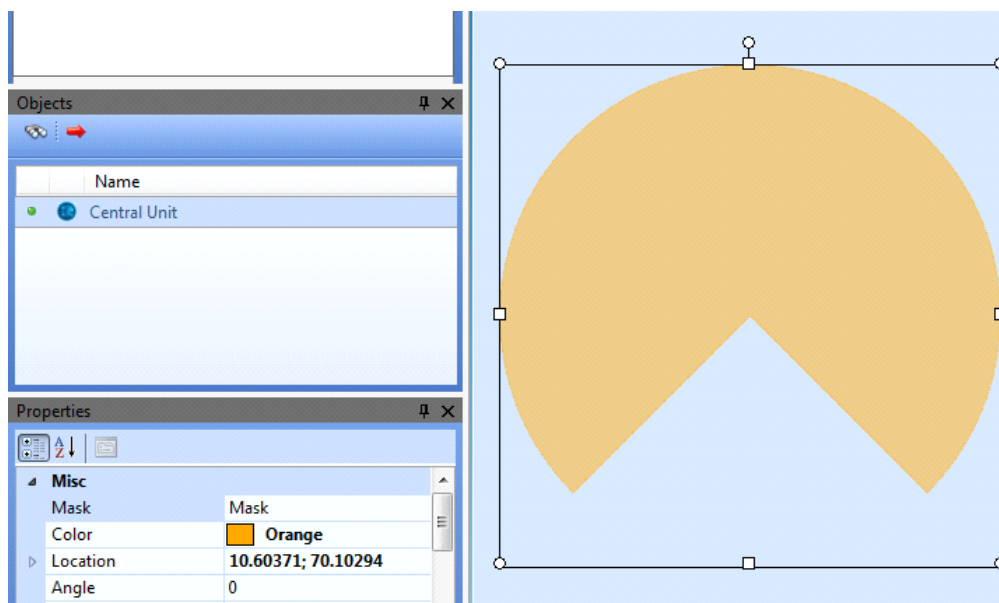


Figure 10-26 Starting the Mask editor

The next window makes it possible to graphically edit the mask. Clicking **Create** will display a snap-to-grid editing grid.

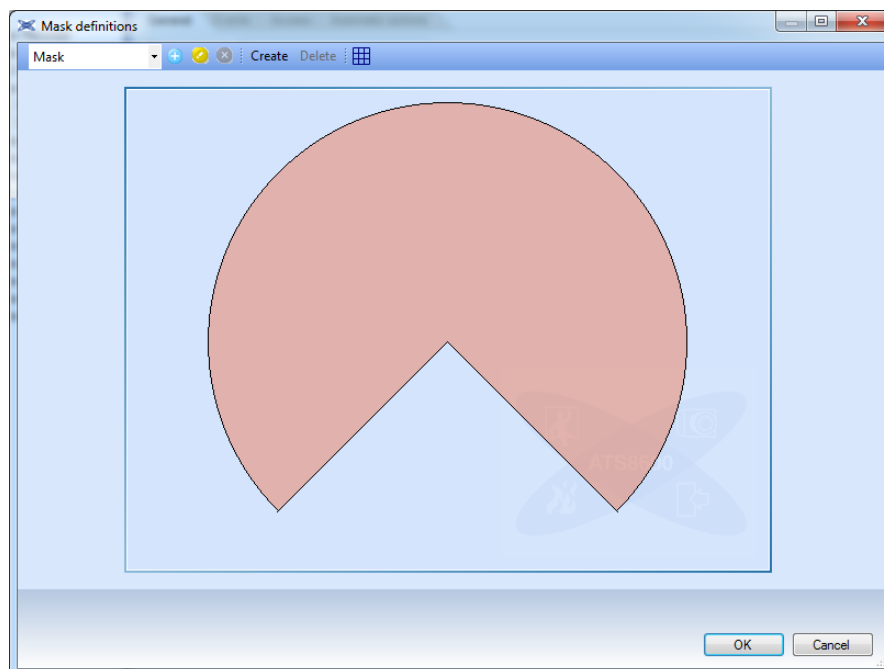


Figure 10-27 Mask editor

Use your mouse to draw a polygon that symbolizes the mask area exempt from being guarded. End the polygon drawing by double-clicking on the last point of the polygon. A green polygon represents an area that is excluded from guarding. Detecting movement in this area will not trigger an alarm. The editor will calculate a hidden, unmasked area for each polygon. This area cannot be guarded because the polygon will shield it from the detection ray. This additionally asked area is marked grey.

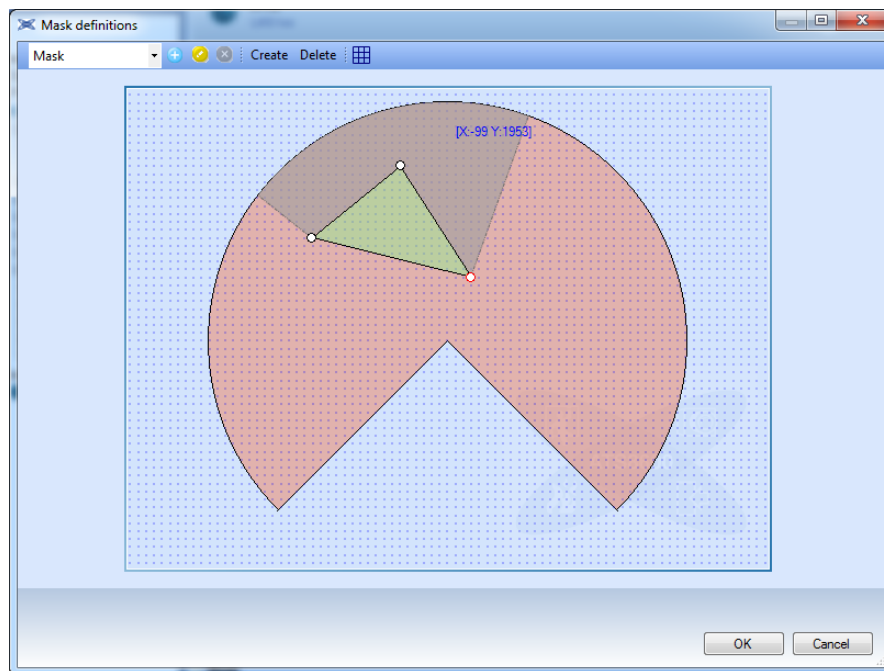


Figure 10-28 Creating a polygon using the editing grid

You can change the position of the created polygon by clicking the given area, holding the mouse and dragging the polygon to the desired position.

If you want to delete the selected polygon, click **Delete**. Alternatively, you can delete the polygon by right-clicking it and selecting **Delete**.

Click  to add a new definition of the mask. Use the scroll-down menu to switch individual masks.

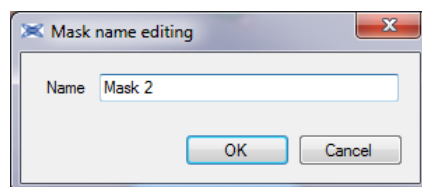


Figure 10-29 Adding a new mask definition

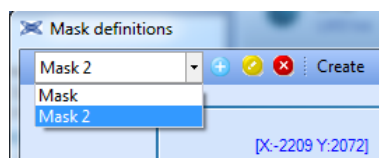


Figure 10-30 Switching mask definitions

Click  to change the name of the currently selected mask. Click  to delete the current mask. The default mask cannot be deleted.

After finishing editing the polygon, close the window by clicking **OK** and save the changes by clicking  **Save** in the *Visualization* panel.

10.7 PTZ module

The *PTZ module* is used to create a link between the detector that is visualized using a mask and the devices that should react to a breach of the guarded area of the given detector. After a breach, the detector sends a command to the specified device (e.g., switching an output).

The *PTZ module* is represented by a special grid that enables definition of individual commands. If you want to display the Link-grid, click  in *Mask editor*.

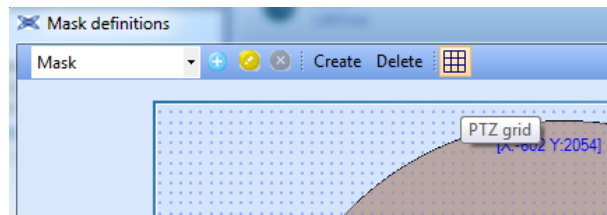


Figure 10-31 Displaying the Link-grid

PTZ grid parameters:

- *width* - number of cells in one row (maximum number: 50)
- *height* - number of cells in one column (maximum number: 50)

10.7.1 Creating a link between the mask and the device

The mask that represents the protected area is divided into a number of smaller cells, indicated by the number of X rows and Y columns. You can define an action for each cell. The action is performed upon breaching the guarded area belonging to the given cell.

The currently selected cell is indicated by a red border. Click  to open the *Devices* tree, select the device to perform an action after a cell breach. Select the command from the list of commands available, or, add a command parameter, if required by the command.

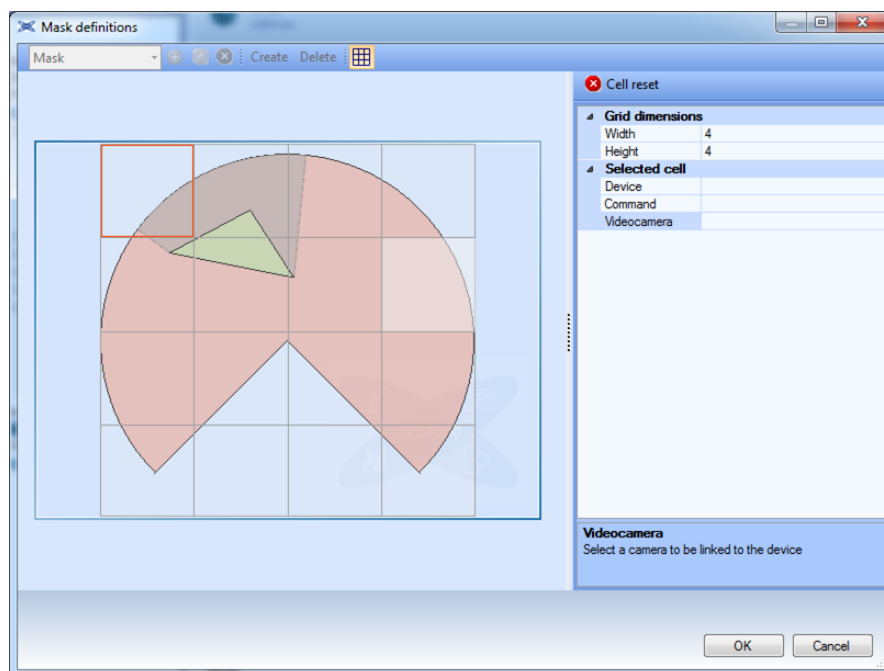


Figure 10-32 Selecting a cell in the PTZ grid

After successfully creating an action, the selected cell is marked with a green dot in its centre.

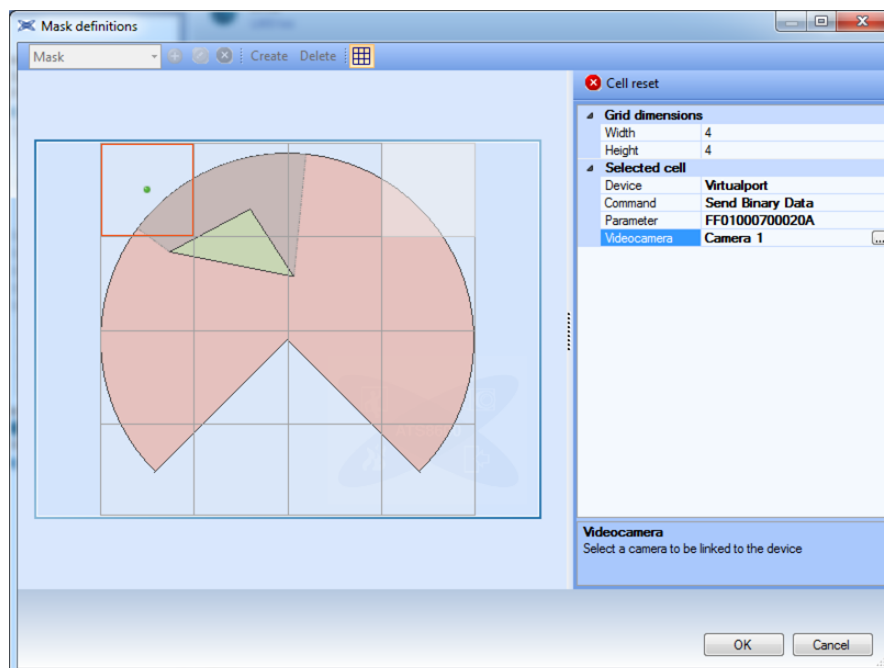


Figure 10-33 Action created for a cell marked with a green dot

If necessary, click the first cell and drag the mouse through the required cells to select multiple cells at once. This way, you can make a rectangular selection. To select additional cells, press **CTRL** and click the required cells. When selecting multiple cells at once, the defined action is added to every selected cell.

To cancel the selection of a cell, press **CTRL** and click the given cell.

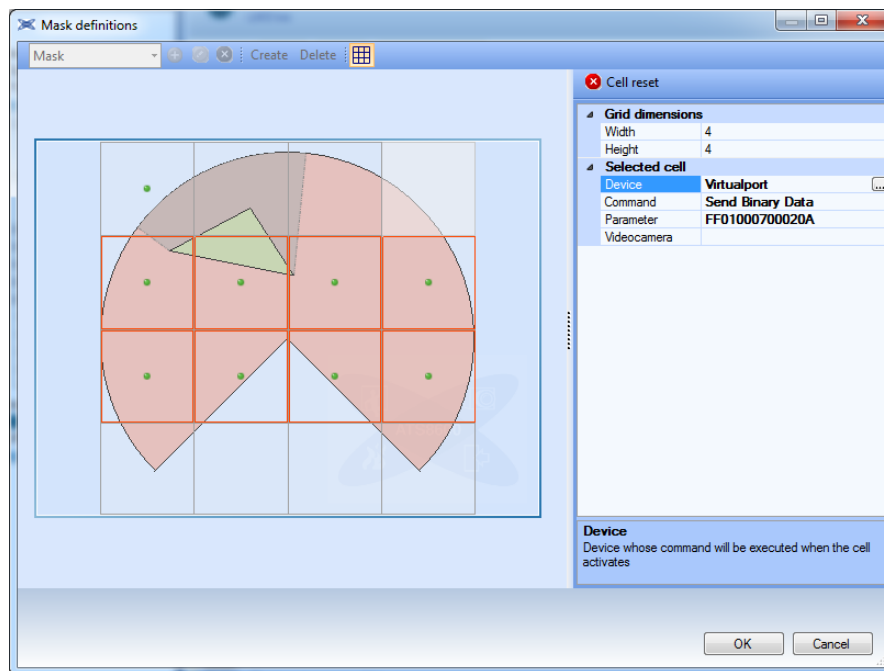


Figure 10-34 Selecting multiple cells

Videocamera can include a reference to the camera directed at the area of the specified cell. When searching for an event in a video record, the record from the camera assigned to the cell, in which that event occurred, is played.

Click  **Cell reset** to reset the selected cell and remove the set action.

To save the performed changes, click  **Save** in the *Visualization* panel.

Note:

In case of a cell breached permanently, the action linked to this cell is performed only once during the defined 10-minute interval. If the breach continues after this interval, the action is performed again.

If an intruder activates one cell, then moves to another and later returns to the first one, all the actions defined are performed in the order, in which the cells were breached, regardless of the amount of time that elapsed between the respective breaches.

If two cells are breached simultaneously and they both have a defined command for the same device, the command coming from the cell with a more severe breach is performed. If the breach severity level is the same, a command to be performed is selected randomly.

11 Monitor

The *Monitor* is the ATS8600 Integrated Security Management System visualization panel and is used to notify users on events in regions and devices.

To activate the monitor select *View - Monitor*.

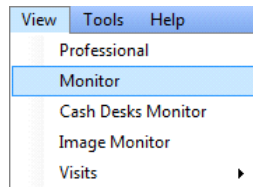


Figure 11-1 Opening the Monitor

Users can select from two different methods for the arrangement of the *Monitor* window in *Personal Settings*.

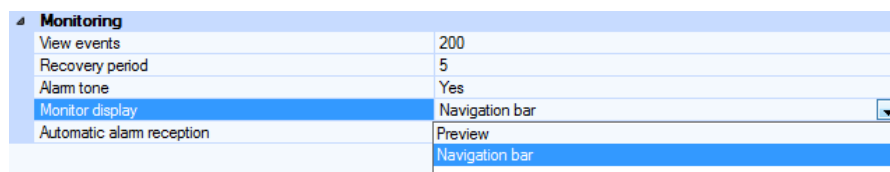


Figure 11-2 Selecting the Monitor view

1. Monitor view in the Preview form

The following *Monitor* window will appear:

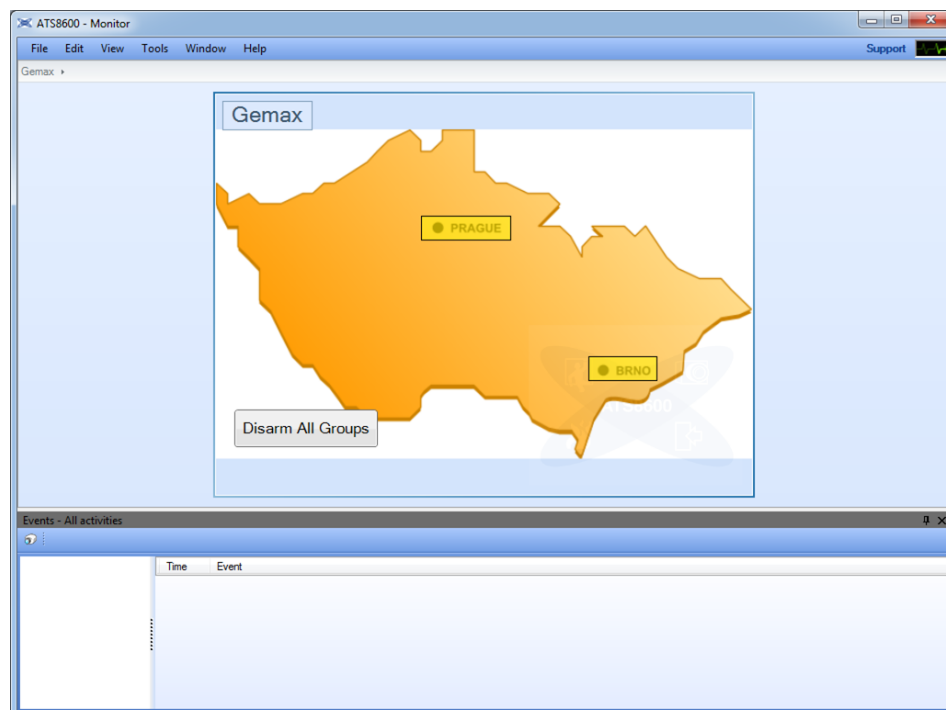


Figure 11-3 Monitor view in the Preview form

According to the structure of the regions it is possible to view them in the form of nesting from higher levels into lower ones. Simply click the element representing the sub-region and the selected subregion and its picture or map will appear in the main part of the *Monitor* screen. The parent region will appear in the smaller window in the left-hand part of the screen. If the active sub-region includes a link to another sub-region (a predefined shape), click it to display the lower level.

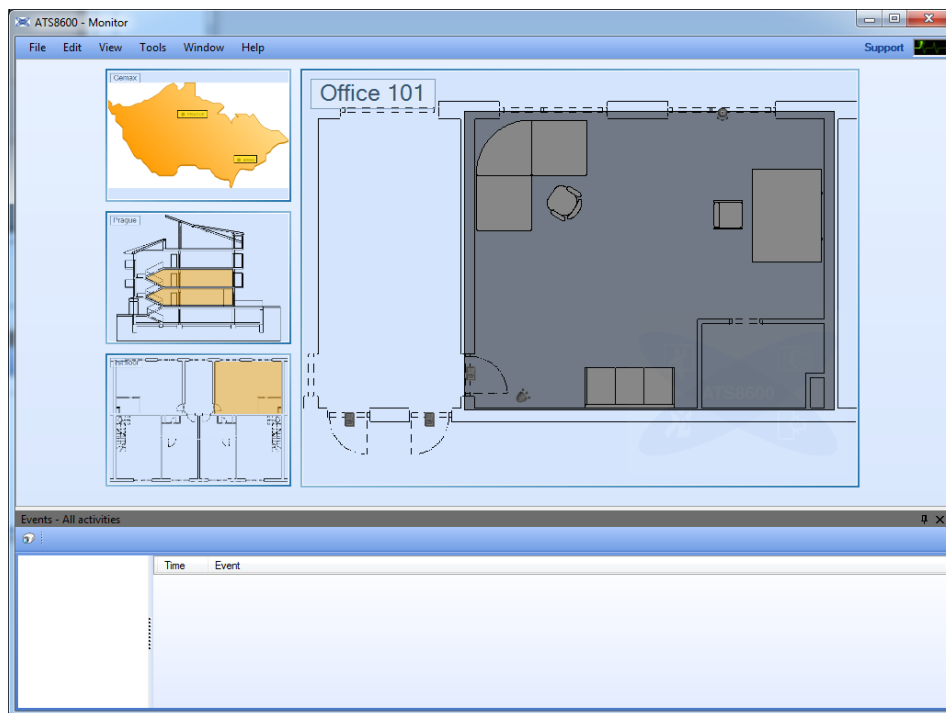


Figure 11-4 Displaying the structure of sub-regions in the Preview form

For this sub-region some devices have been added into the *Visualization*, which are actually located in that region.

2. *Monitor* view in the *Navigation bar* form

The *Monitor* window opens and has a slightly different structure than the *Monitor* in *Preview* form. The selection of regions and subregions is performed by means of selecting the required region structure in the *Navigation bar* of the window.

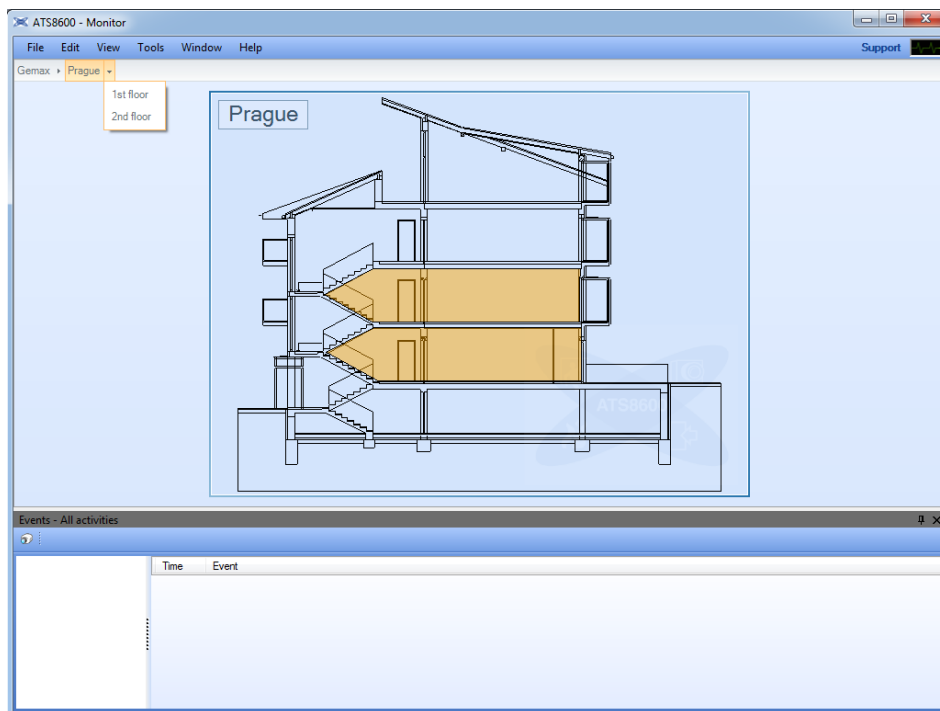


Figure 11-5 Monitor view in the Navigation bar form

The *Monitor* serves to monitor individual ATS8600 Integrated Security Management System regions and devices, their status, warnings, alarms and provide remote control options. As the regions represent a true part of the system the devices in the regions provide the real conditions, the user responsible for monitoring has a quick and comfortable monitoring tool. As soon as a device detects an event, alarm notification in the highest parent region is initiated. The map guides the user when identifying a particular device that detected the event.

Issuing remote commands to devices happens in a similar way as in the *Devices* and *Regions* trees. Right-click the icon of the chosen device and select the command to remotely control a device.

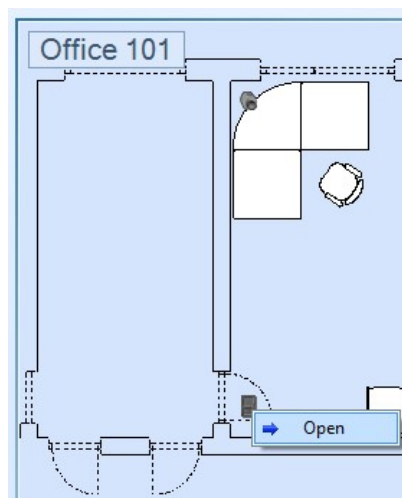


Figure 11-6 Issuing a command on a device

After performing the issued command, the changed status will be indicated also by a changed device icon; e.g., if a command is issued to open a door, the door icon will change into the open door icon.

11.1 Monitor panel windows

The *Window* menu includes additional event windows available in the *Monitor* view. Selecting a window type will open the selected window and show it in the panel. You can open several windows. The window layout is saved such that after application restart the monitor shows the same layout.

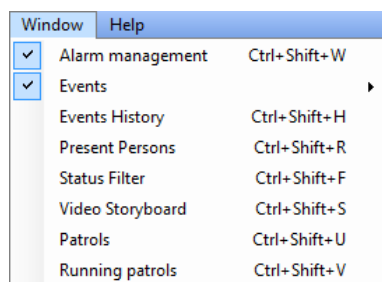


Figure 11-7 Window menu

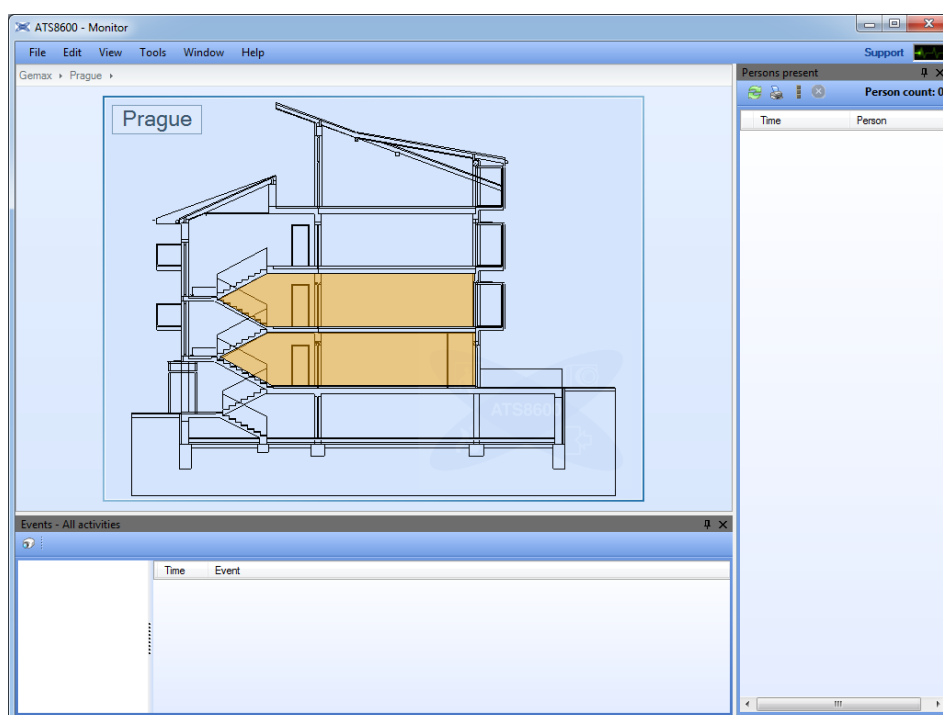


Figure 11-8 Open windows: Events and Persons present

11.1.1 Events window

You can view all events recorded in the ATS8600 Integrated Security Management System in the *Events* window.

You can open the window from the menu and click the respective icon to pin it in the upper right corner. It will thus remain open in the *Monitor* panel. Else the window will hide automatically if another window becomes active.

The *Window - Events* drop-down menu contains different event filters that the logged-in user has permission to view. Multiple event windows can be open simultaneously whereas each window has different filtering criteria. The system enables the users to create defined event filters ([see chapter Event filtering](#)).

When viewing the events in the *Monitor* window, the person related to this event has no photograph. The photograph appears only if the event is related to a person who has a photograph in their personal profile.

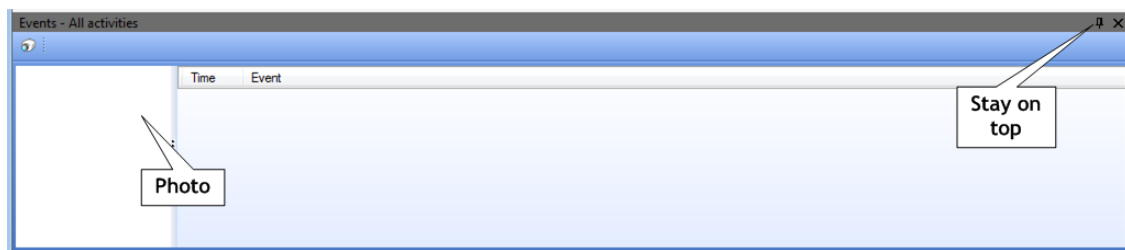


Figure 11-9 Events tab open

Tip:

We recommend to pin the *Events* and *Persons present* windows in the *Monitor* panel, if you wish to hide them temporarily. Click X to close the window. You can reopen it from the menu.

11.1.2 Event history window

The *Event history* window allows users to view the history of events related to the selected region. Compared to *Events*, it provides an overview of past events, as well as the ability to search events according to selected criteria.

Moreover, some events are linked to devices that are visualized in one of the regions. After selecting such an event, a Go To button appears in the window. After clicking this button, on the main *Monitor* window appears the region that contains the device that raised the event. The given device remains selected for a few seconds to make it easier for the user to identify. This feature is useful when you need to display an event in a region that requires immediate resolution, such as an alarm.

If the element is visualized in multiple regions (e.g. the parent region and the sun-region below), you can select the required region. Just click the drop-down menu that is placed right next to the button. The element cannot exist in multiple places at once. However, the same region is may be visualized multiple times. This is done in order to have multiple views for the devices (e.g., map, logical, or for guards or technicians).

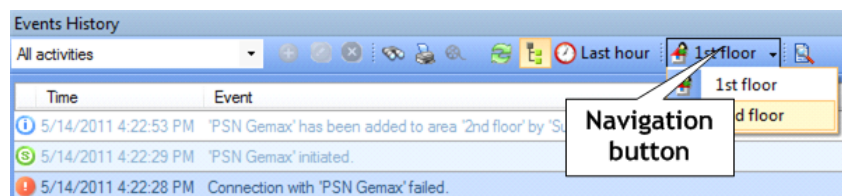


Figure 11-10 Event history

11.1.3 Alarm management window

The previous two windows provide a view on all types of events that occur in the ATS8600 Integrated Security Management System. The system management typically does not deal with all of them, however. Instead, it focuses on the so-called "critical events" (e.g., alarms, device errors). To improve the process of dealing with these events use *Alarm management*, which links Event records to records of the actions used to fix the events.

A typical procedure for dealing with an alarm event is as follows:

- I. An event happens. .
 - The event appears in the *Alarm management* windows as a new record.
- II. The dispatcher or guard notices the new alarm event and takes required action.
 - The dispatcher or guard adds a record stating that the event has been noticed. The time when the problem has been noticed For the first time is also recorded.
- III. The event is resolved by the dispatcher or guard .
 - Notes concerning the resolution can be added. They are stored with the event.
- IV. The problem is resolved.
 - The dispatcher or guard marks the problem as resolved and it disappears from the *Alarm management* window.

Just as with the majority of actions within the system, before using the functionality, it is necessary to set permissions for the user (typically a dispatcher or guard). Detailed description of setting permissions are described [in chapter Permissions management](#)).

1. At first, you need to identify the person who should receive the permissions.
2. In the *Permissions* tab, select *Application* from the drop-down menu.

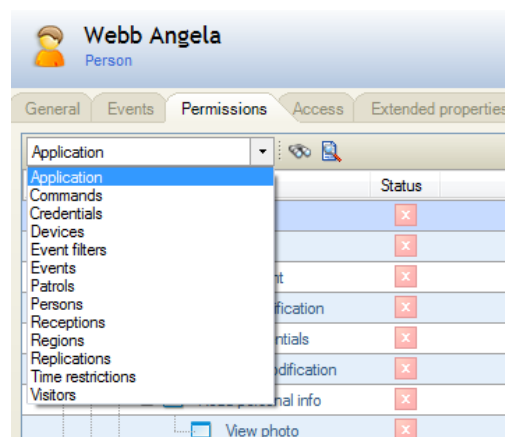


Figure 11-11 Setting the application permissions

3. In the selected tree, go through *Root -> Application -> Visualization -> Monitor* and then to the *Alarm management* and *Resolve alarms* nodes.



Figure 11-12 Permissions setup

A person can have two types of permissions:

a. Alarm management

Enables the person to view the Critical Events list in the *Alarm management* window. The person can acknowledge the event and add notes to it.

b. Resolve alarms

Enables the person to mark problems as resolved. This permission relies on functionality that is provided by *Alarm management*. Therefore, it should be set up together with the previous entry.

The *Alarm management* window is used to process events that need immediate resolution, like following:

I. A new event appears. Select it to start processing the event

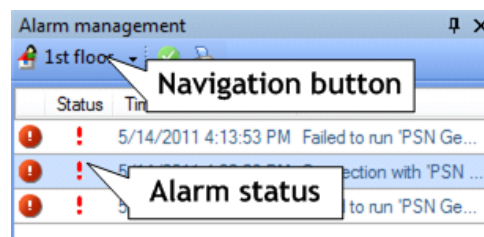


Figure 11-13 Alarm management

II. You can click the region if available which moves you to the region containing the device that delivered the event ([see chapter Event history window](#)).

III. You decide to investigate the event. Start the Failure dialog by taking one of the following steps:

- i) double-click the Event in the list, or
- ii) pressing .

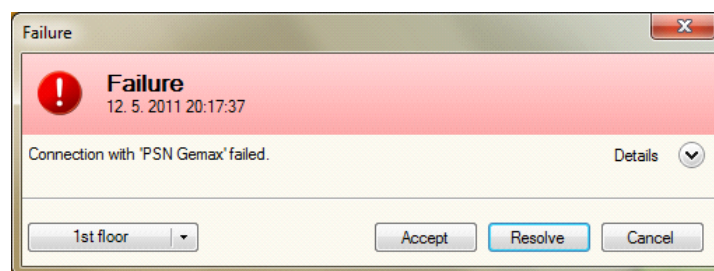


Figure 11-14 Failure dialogue box

IV. In the Failure dialog, click **Accept**. The following happens:

- i) "Alarm accepted" is automatically logged, together with the time and date stamp. A list of notes can be viewed after clicking **Details**.
- ii) The event status changes from  to .
- iii) The **Accept** button is now greyed out. An Event can only be accepted once. If the *Alarm management* module is used by several users simultaneously, the **Accept** button is greyed out for other users as well. However, the dialog box (including the sound signals) remains present in the

Client stations, despite the fact that the alarm has already been accepted by another User. Therefore, other users can add their own notes on the alarm or close the dialog without any resolution.

iv) Click the  icon in the alarm or *Alarm management* window to open and print emergency guidelines, which can be helpful when solving a critical event.

V. You cannot deal with the failure on your own; therefore, you add a note:

"Installer called to request support visit."

Go to the Failure dialogue again and press **Details**. Type the text into the Note box and press **Add**.

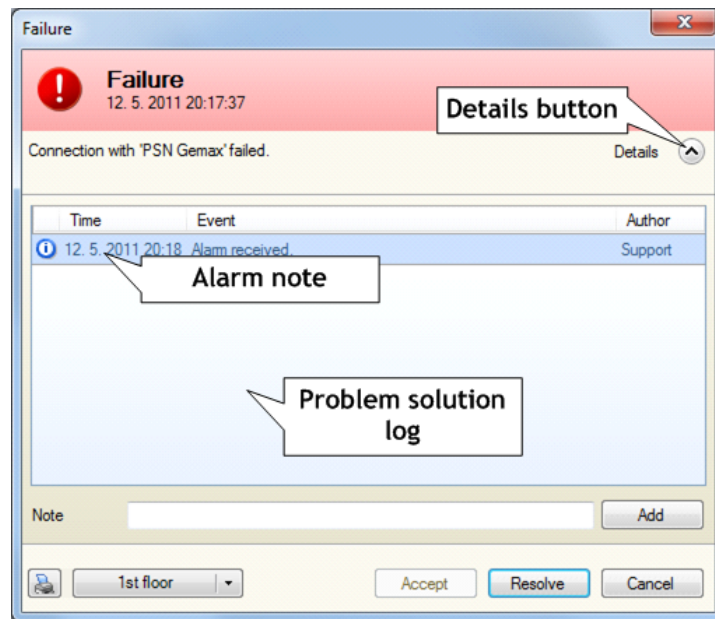


Figure 11-15 Alarm details

VI. The day after the repair, go to Failure and click **Resolve**. Note stating "Alarm resolved" is shown and the event disappears from the *Alarm management* alarm list. Click **Resolve** to save the current draft note to the alarm.

If necessary, you can review the problem solution log. A log sub-window appears after selecting the critical event in any window containing *Events* and pressing **Details**. This window contains the complete log with the problem's solution.

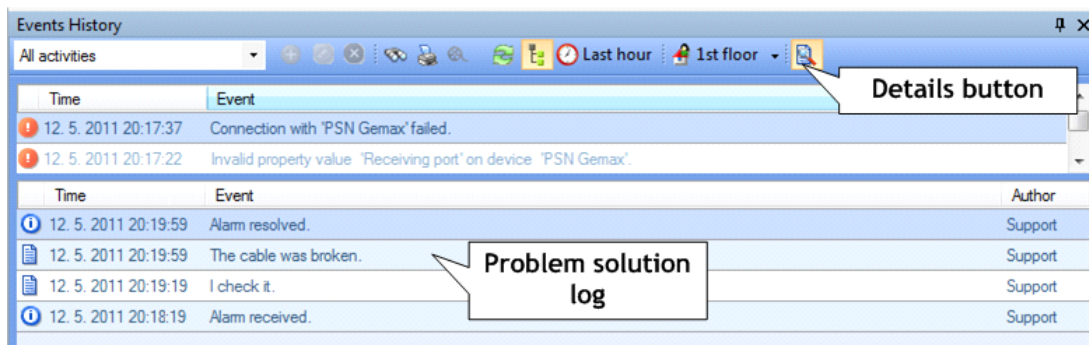


Figure 11-16 Displaying the problem solution log

Warning:

The dialog box appears under two conditions:

- a) the *Alarm management* module is on - [see chapter Overall enabling or disabling of Alarm management](#).
- b) the user has application permission *Alarm management* - [see chapter Types of permission](#).

Note:

At the level of the same time, only one dialog box can be displayed. When an alarm dialog is already open and another alarm occurs, the other alarm is logged only in the alarm list. The alarm dialog of the new alarm is displayed only upon closing the previous alarm dialog box.

11.1.4 Persons present window

The method for counting present persons is described in detail [in chapter Number of persons in the region](#).

To display the window with an overview of persons present, click *Window - Persons present* in the *Monitor* panel.

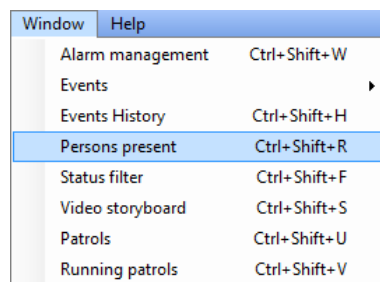


Figure 11-17 Displaying the Persons present windows

11.1.5 Status Filter window

The function of the *Status filter* window is described [in chapter Device statuses filter](#).

11.1.6 Video storyboard window

The *Video storyboard* window allows you to play video footage from a selected event.

To play event videos:

1. If you want to show the video from an event, search for the event in the *Event history* window.
2. Double-click the event to move the exact date and time of that event to the *Video storyboard* window.
3. For the selected time, select the camera from which you want to view the video stream.
4. If *Video storyboard* is open, play the video by right-clicking the selected camera and selecting *Record playback*.

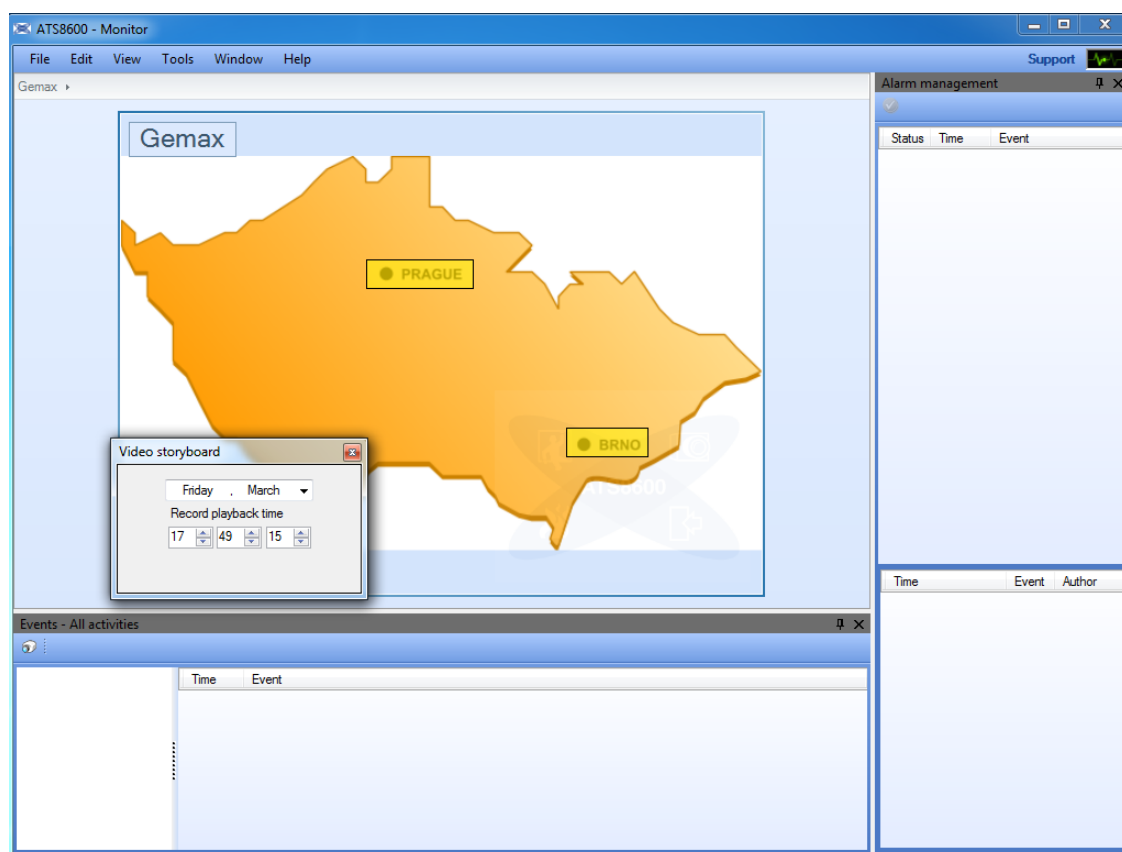


Figure 11-18 Video storyboard

Using this function you can play video footage from multiple cameras for the same time - you can see what was happening at a certain point in time in all regions of interest. One example would be a robbery. You can watch the scene of the robbery from the camera in the shop but also what happened at the entry door or in the any other part of the shop where camera's are located.

11.2 Alarm sounds

If the user selects audible signalling on alarms, an alarm will sound in addition to visual alerts. To set alarm tones, select the option in the *File* menu in the Monitor window. Thus, the dispatcher responsible receives prompt notification and accurate information on the device status in the respective region.

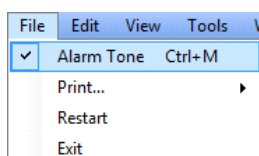


Figure 11-19 Alarm sounds active

11.3 Device Remote Control

Another property is the remote control of devices, similar to the *Devices* and *Regions* trees. Right-click the icon of the chosen device and select the command to control the device remotely.

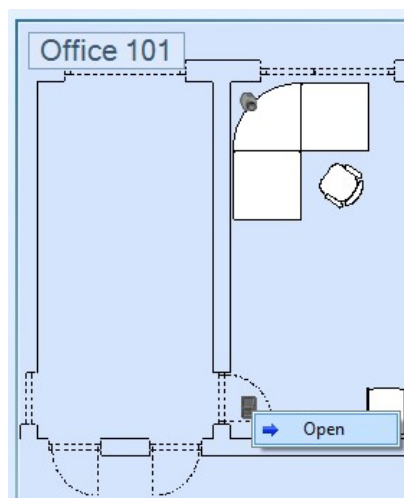


Figure 11-20 Issuing a command on a device

Upon performing the command, the device icon changes as well, indicating the change of the status directly. For example, in case of the command to open a door, the door icon changes to the open door icon.

11.4 Connecting a camera to a device

Causing an alarm on the device always has the same response: The operational staff has to investigate and resolve the Event immediately. Even though it is easy to find the region where the event originated from ([see chapter Event history window](#)), additional information to further investigate is appreciated. If the region is monitored by a camera system, you may want to only view the video footage from the camera that raised the event. A region or even more a system is often full of camera's. Looking for one particular camera is a time-consuming task, especially when there are multiple cameras in the region.

The only information you have is the position of the device that caused the alarm. It is useful to link detection devices, such as intrusion detectors with cameras that cover the same field of view. This link also enables the use commands, such as **Show/Record playback** directly from the context menu of the linked devices. The video feed from the camera monitoring the element in question is displayed immediately. You no longer need to browse the full list of camera's and look for the camera that "could have seen" the cause of the event.

You can use the *Devices* tab of the *Professional* panel to logically pair the signalization devices and cameras.

To do this, use the following steps:

1. Go to the *Professional* panel and click the *Devices* tab.
2. Select the device that you want to link to the camera.
3. In the *General* tab, search for the *Camera* field and click it.
4. The  button appears on the right side of the field. Click it.

5. A window with all cameras, defined in the *Devices* tree appears.
6. Select the camera that monitors the signalization device.
7. Click **OK** and press **Save**.

Now you are able to use **Show** , which begins to play the camera's live feed, or **Record playback** , which plays a recorded video feed starting at a requested time ([see chapter Video storyboard window](#)).

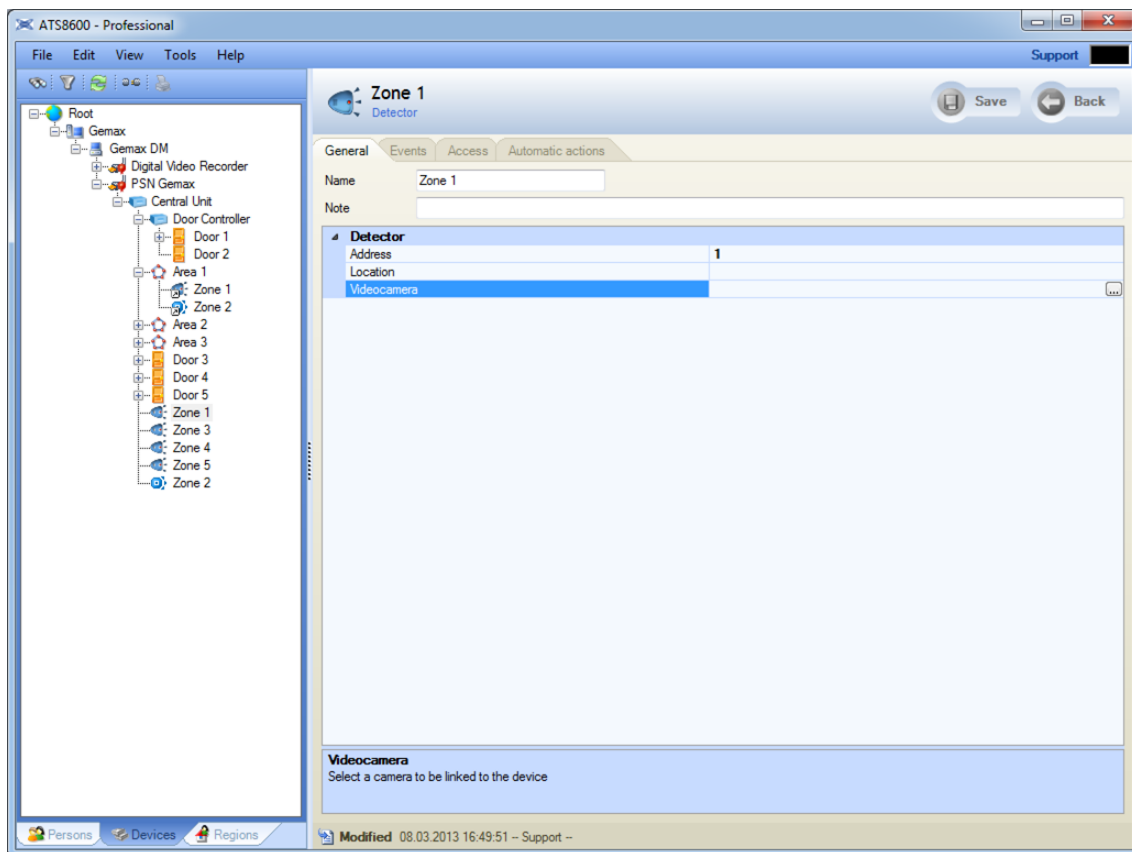


Figure 11-21 Pairing a camera with a signalization device

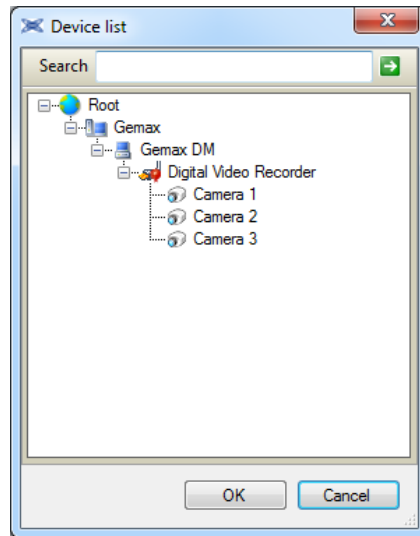


Figure 11-22 Settings function
The window with cameras

11.5 Automatic Camera Live Screen View in the Monitor Panel

Once the event has been delivered from the signalization device connected to this camera, you can view the camera live screen in the *Monitor* panel. The following example illustrates the practical usage of this functionality:

1. Set the connection of the camera with the signalization device ([see chapter Connecting a camera to a device](#)).
2. Create an event filter for those event types that initiate the automatic camera live screen view ([see chapter Event filtering](#)). Because every event opens a new window containing a video, we recommend setting the filter terms to prevent the events from bulking in the filter after a very short time.

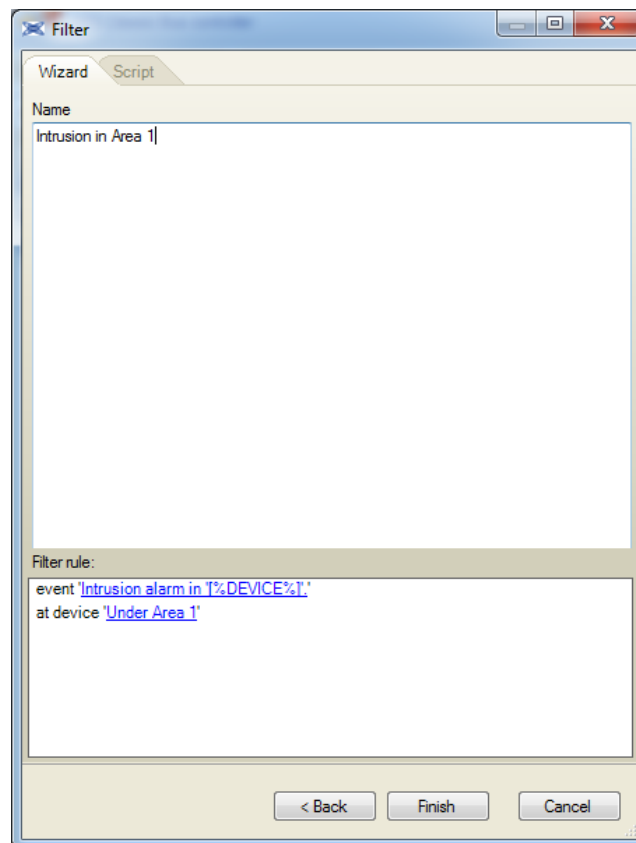


Figure 11-23 Creating an event filter for the alarm-type events

3. Open the newly created filter in the *Monitor* panel and click the  icon.

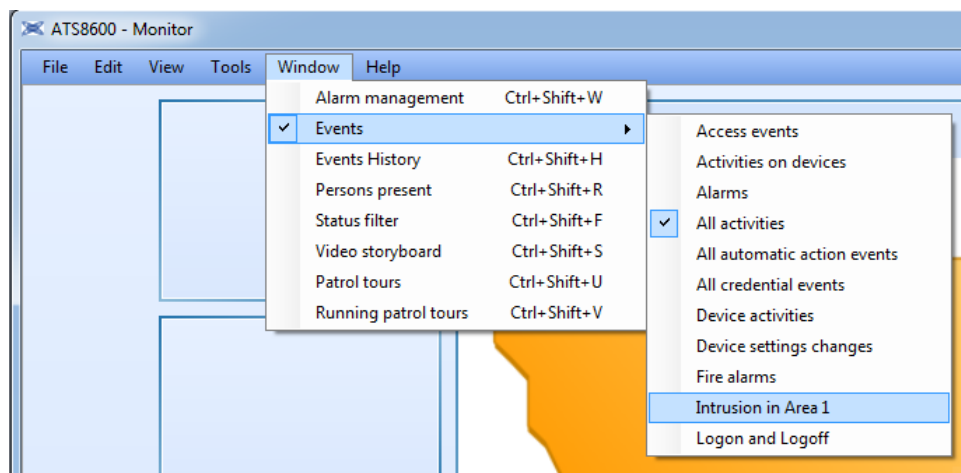


Figure 11-24 Turning the newly created filter on

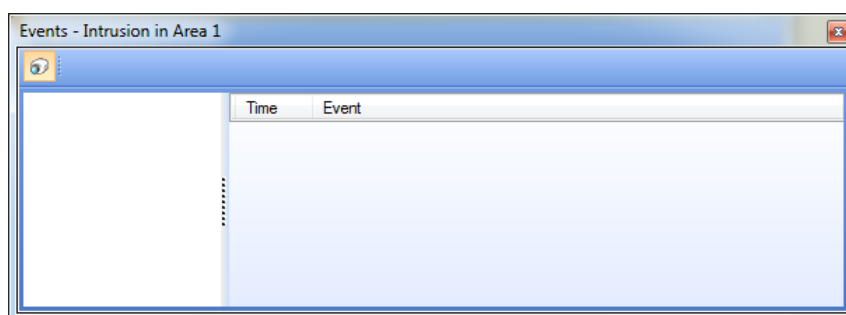


Figure 11-25 Active automatic camera live screen view

4. The camera live screen view is activated upon the delivery of an event from the signalization device connected with the camera.
5. The staff analyze the incident and, after it has been resolved, they close the window containing the video.

Warning:

The application behavior depends on the camera system type, which means that technical issues concerning the query camera video library may occur (slow reactions of the application during the video initialisation, heavy workload of the computer hardware resources when the camera is open, incorrect view of several cameras simultaneously, etc.)

11.6 Controlling PTZ Cameras

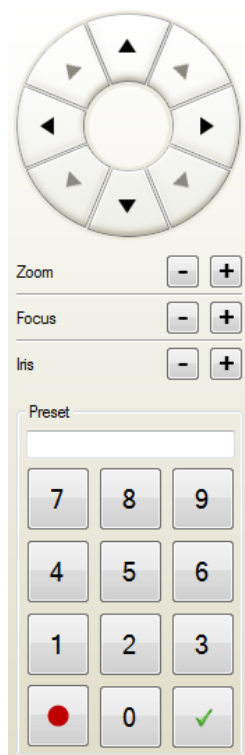


Figure 11-26 PTZ control interface

By opening the live image from a PTZ camera, a control bar opens in addition to video.

Use direction buttons on the bar to change the direction of the camera. Click and hold the button of the required direction. Release the direction button to stop the camera from turning.

buttons allow to set zoom, focus and iris of the camera. To rotate the camera to a preset position enter the respective preset number on the virtual keyboard and click . This way only preconfigured preset positions can be selected.

To save the current position of the camera as a preset position click , enter the number of the required preset position and click to save. The scope of numbers of available preset positions depends on the connected device.

11.7 Overall enabling or disabling of Alarm management

The administrator is eligible to enable or restrict *Alarm management* in the whole system. This is done as follows:

1. Select *Tools* from the *Settings* menu.

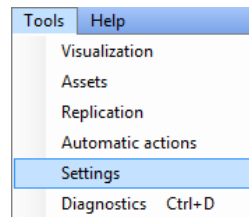


Figure 11-27 Function Settings

2. After displaying the *Settings* window, go to *System settings* and click *System settings*.
3. In the displayed *Alarm management* , you can enable or disable marking events as alarms.

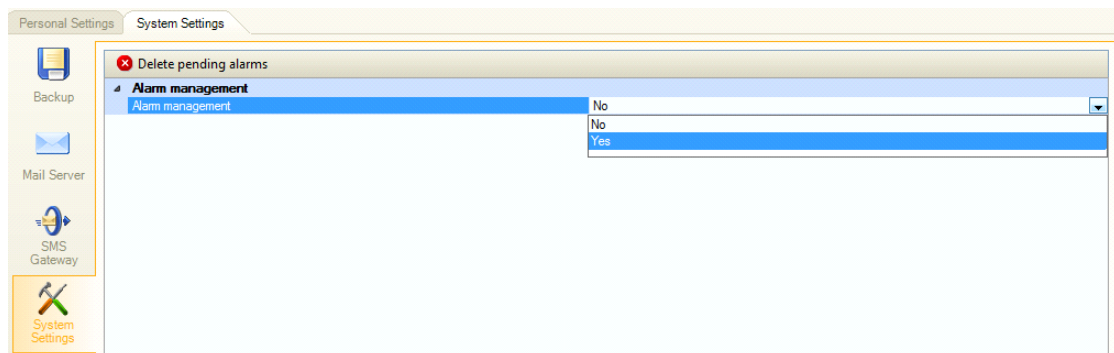


Figure 11-28 Alarm management

If *Alarm management* is set, users are notified about alarms in the *Monitor* panel and a record of unresolved alarms is kept.

If disabled, alarms are not created.

12 Image Monitor

Image Monitor enables the users to check persons accessing buildings, rooms, devices, etc. Each person who uses a credential at a reader will be displayed at the *Image Monitor* panel. Else the window will hide automatically if another window becomes active. This function provides additional information and an option to verify whether the credential was used by the authorized person or whether it was misused (e.g., stolen).

For full usage of *Image Monitor*, the user can add a photograph to each person.

Note:

Importing a photo for a person is described [in chapter Adding a picture to a person's record](#).

You can find *Image Monitor* in the *View* menu.

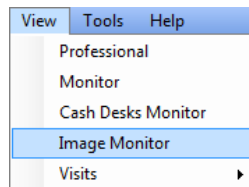


Figure 12-1 Image Monitor in the View

Open the *Image Monitor*, the  icon appears with the option to select a door that is present in the building.

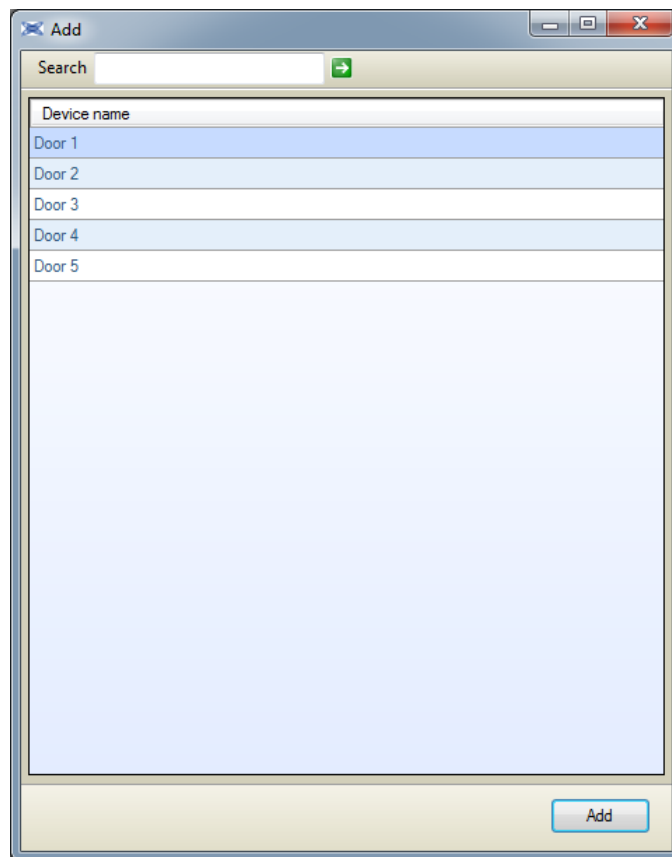


Figure 12-2 Selecting a door

Note:

You can select multiple doors by pressing and holding *CTRL* and selecting the individual doors.

Image Monitor can display the photos of the last four persons that entered the building.

The last entry is displayed in a large frame and is placed into the upper queue, in the moment of the next entry.

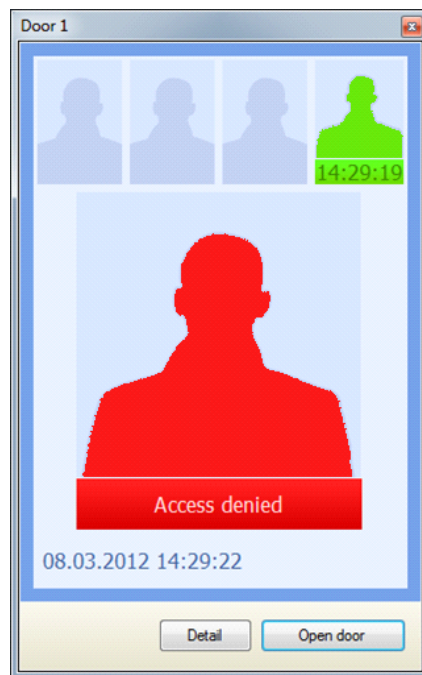


Figure 12-3 Displaying the last four entries with a photo

If the user does not assign a photo to the person, a silhouette appears instead.

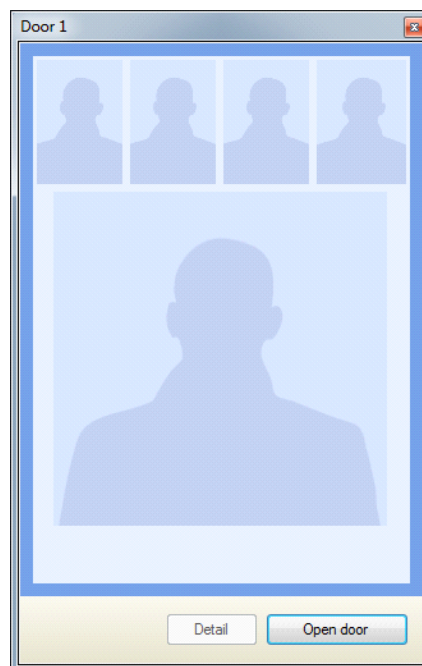


Figure 12-4 Silhouette

If the person is authorized to enter the building, the photo/silhouette turns green, accompanied by a sound.

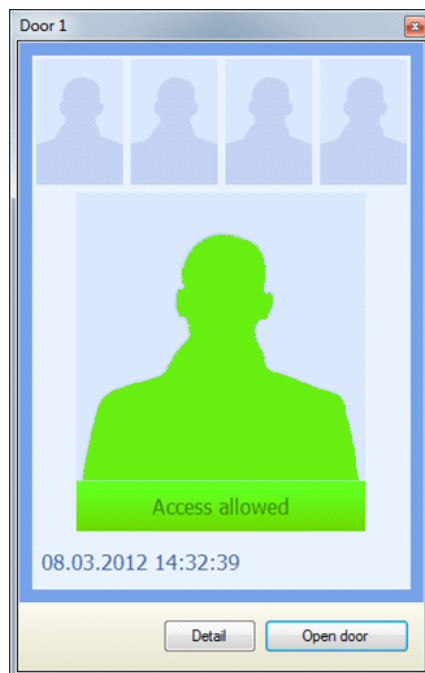


Figure 12-5 Photograph - Access permitted

If the person is not authorized to enter the building, the photo/silhouette turns red, accompanied by a sound.

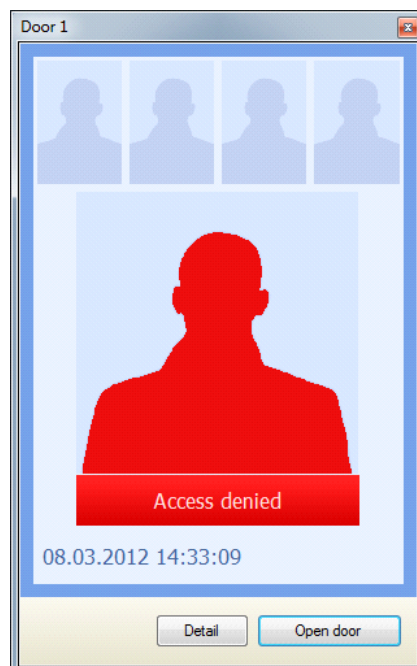


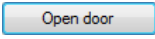
Figure 12-6 Photograph - access denied

If the person is authorized to enter the building during a set time interval and is trying to enter the building at a different time, the photo turns yellow, accompanied by a sound.

Note:

Time restrictions set-up is described [in chapter Time Restrictions](#) and entering the start date and end date of employment is described [in chapter Entering start date and end date of access](#).

The Open button

It is okay to run the  to open the door directly.

The Detail button

Click  or double-click the photograph to obtain basic information about the person:

- Time and date, door name and transaction result
- First name and surname
- Address
- Identification Card
- Validity (time period)

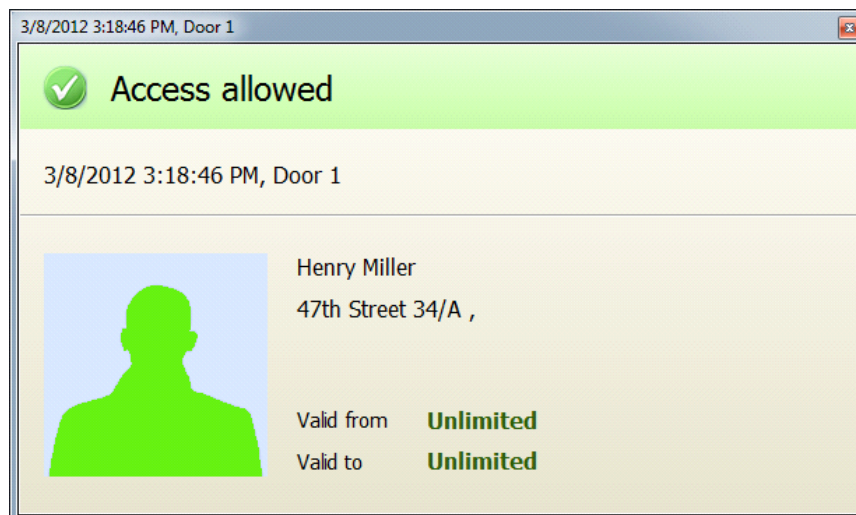


Figure 12-7 Details of a person with allowed access

13 Patrol tours

Patrol tours allows to plan patrol tours of guards in a given region. The system manages these patrol tours. If a guard during a patrol tour does not perform a verification within a previously defined time interval, the system activates an alarm in ATS8600. Performing the verification means using cards or PINs or any other valid identification device to allow the system to identify the guard.

13.1 Creating and modifying a patrol

Creating a new patrol tour and its subsequent modification can be performed in *Visualization*. Click the *Window* menu and select *Patrol tours*.

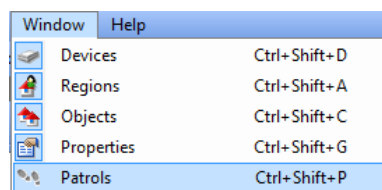


Figure 13-1 Starting the patrol tours editor

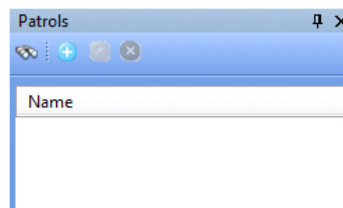


Figure 13-2 Patrol tours editor window

Patrols editor contains several command controls:

- text search in the patrols list
- create new patrol tour
- edit the selected patrol tour
- delete the selected patrol tour

Clicking creates a new patrol tour. Enter the tour name and add checkpoints. Turn on the *Devices* tree and drag selected objects that would be recognized as patrol checkpoints. By clicking , you return to the tours list.

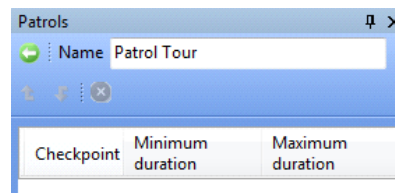


Figure 13-3 Creating a new tour

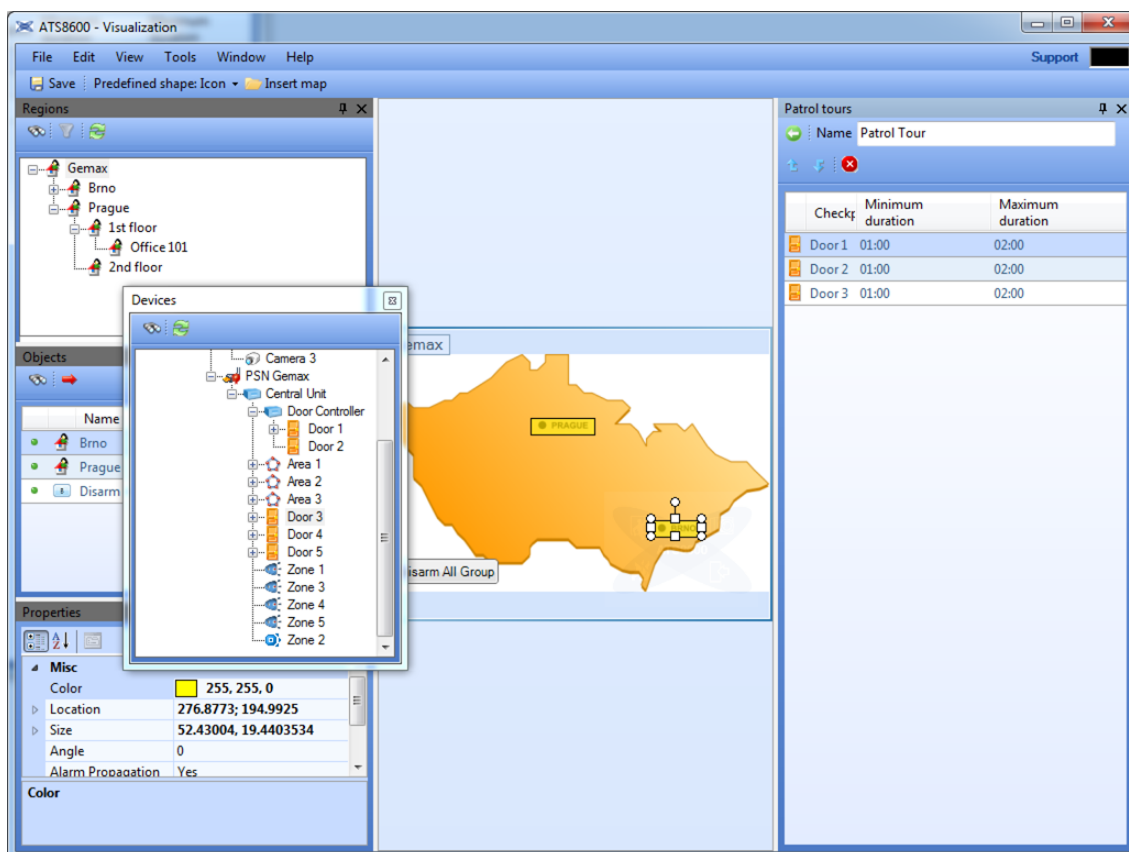


Figure 13-4 Adding checkpoints to patrol tour

Warning:

The following devices can be added to the patrol tour as checkpoints: *door* and *keyboard*.

Each checkpoint must have a set maximum and minimum time duration, during which a person must move from the previous point to the new point. At each checkpoint the credential for that person needs to be entered (PIN) or badged in front of the reader.

By using  and , you can move the selected checkpoint up or down the list. Clicking  deletes the selected checkpoint from the patrol tour.

After editing the tour, save the changes by clicking  in the upper-left corner of the application.

Note:

A patrol tour can contain one checkpoint multiple times. In that case, the person must go through it multiple times in the defined order.

13.2 Starting and monitoring a patrol tour

You can start and monitor the created patrol in the *Monitor* panel. Else the window will hide automatically if another window becomes active. If you want to view the list of available patrol tours, start *Patrols* window.

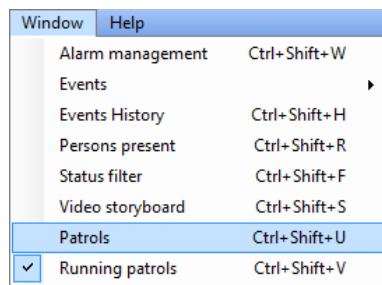


Figure 13-5 Enabling a panel Patrols

Click the patrol tour name and click  to start the patrol tour.

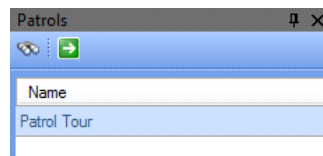


Figure 13-6 Starting a patrol tour

When starting a patrol tour, you need to select a person that will perform the patrol tour. In an open window enter the person name and click . After selecting a guard from the guard list and clicking **OK**, the patrol tour will start.

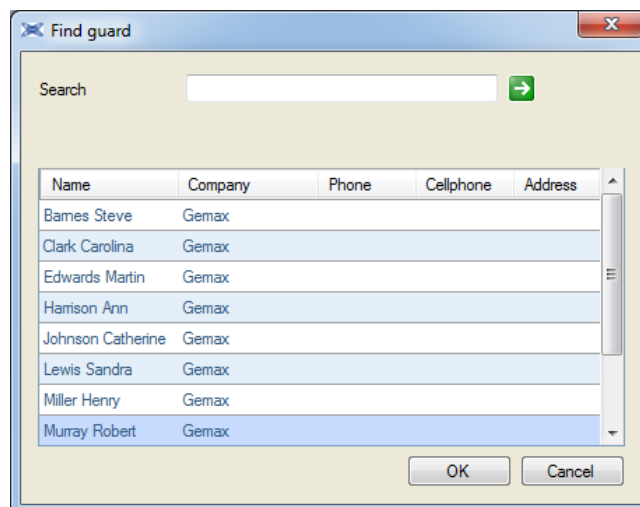


Figure 13-7 Selecting a guard to perform a patrol tour

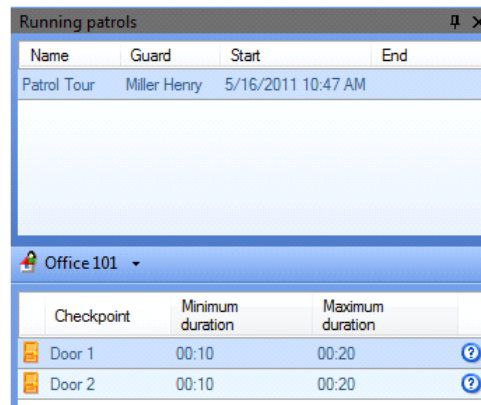
A running patrol tour can be monitored using the *Running patrol tours* panel. Else the window will hide automatically if another window becomes active. The panel can be launched in the *Monitor* panel via the *Window* menu.

The *Running patrol tours* window has two sub-windows:

- the upper part contains a list of all running patrol tours, the name of the person who performs the patrol tour, and the start and end time of the patrol.
- the lower part contains a detailed list of checkpoints of the selected patrol tour, including a maximal and a minimal duration. After every checkpoint, its status is marked and is based on the patrol tour.

Checkpoint can have the following statuses:

- ❓ - the checkpoint was not passed and the maximal duration has not yet expired.
- ✅ - the checkpoint was passed within the time duration.
- ⚠️ - checkpoint was not passed within the maximal duration.



The screenshot shows a window titled "Running patrols" with a table of patrol tours and a list of checkpoints. The table has columns: Name, Guard, Start, and End. The first row is "Patrol Tour" with Guard "Miller Henry" and Start "5/16/2011 10:47 AM". Below the table is a dropdown menu for "Office 101". Underneath is another table with columns: Checkpoint, Minimum duration, Maximum duration, and an icon column. The first row is "Door 1" with "00:10" and "00:20" and a question mark icon. The second row is "Door 2" with "00:10" and "00:20" and a question mark icon.

Name	Guard	Start	End
Patrol Tour	Miller Henry	5/16/2011 10:47 AM	

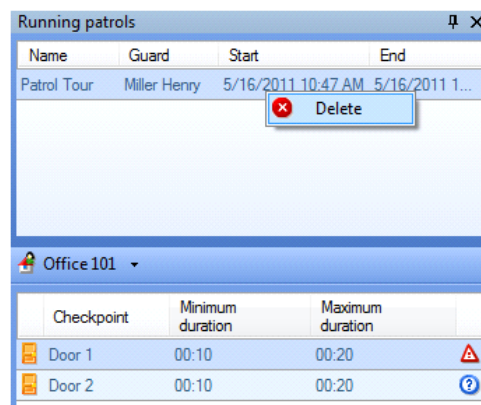
Office 101 ▼

Checkpoint	Minimum duration	Maximum duration	
Door 1	00:10	00:20	❓
Door 2	00:10	00:20	❓

Figure 13-8 Started patrol tour with the name of the guard and the checkpoint list

If the guard arrives at a checkpoint before the minimal duration, a early arrival event is logged into the system and the patrol tour continues.

If the guard is not identified at a checkpoint before the maximal duration elapses, the system will start an alarm and log an unsuccessful patrol tour event. In that case, the user must manually delete the patrol tour from the *Running patrol tours* list.



The screenshot shows the "Running patrols" window with a "Delete" button highlighted over the "Patrol Tour" row. The "End" column now shows "5/16/2011 1...". The "Door 1" checkpoint now has a warning icon (⚠️) instead of a question mark, and "Door 2" still has a question mark icon.

Name	Guard	Start	End
Patrol Tour	Miller Henry	5/16/2011 10:47 AM	5/16/2011 1...

Office 101 ▼

Checkpoint	Minimum duration	Maximum duration	
Door 1	00:10	00:20	⚠️
Door 2	00:10	00:20	❓

Figure 13-9 Unsuccessful end of a patrol tour and its manual deletion from the Active patrol tours list

If the guard passes all checkpoint between the minimal and maximal duration, the system logs a successful patrol tour end event and that patrol tour is automatically deleted from the *Running patrol tours* list.

If the checkpoint device has a camera assigned to it, the user can view a live feed from the camera by right-clicking the checkpoint in the *Running patrol tours* list.

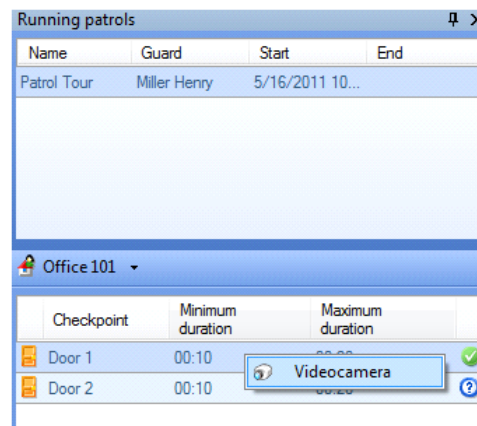


Figure 13-10 Displaying the camera feed during patrol tour monitoring

If the device in the selected checkpoint is visualized in a region, clicking the button with the region name in the *Running patrol tours* window will display the region that contains the device. The checkpoint's position on the ground plan will flash.

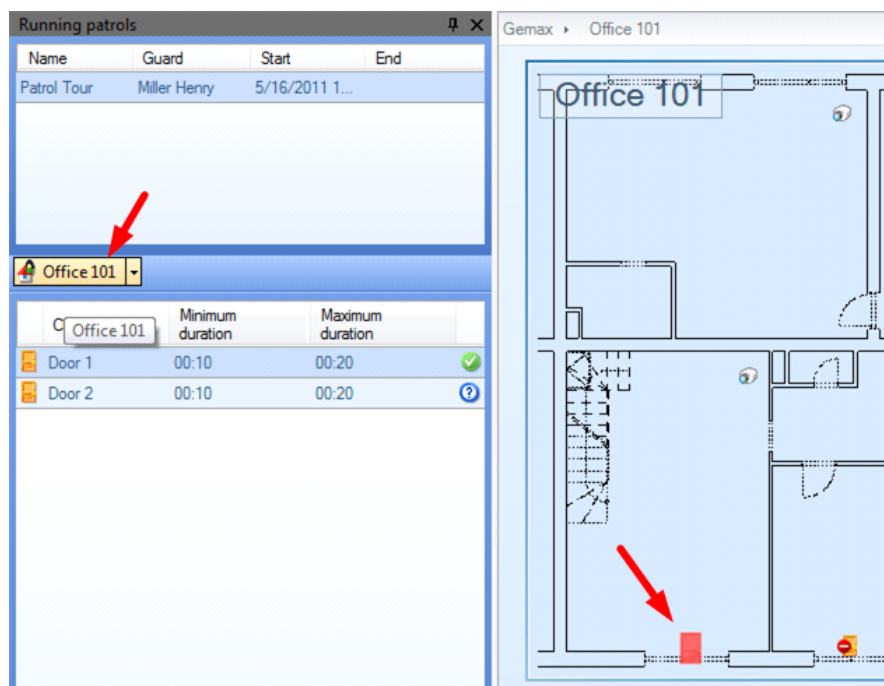


Figure 13-11 Displaying the checkpoint on the map

14 Cash Desk Monitor

If ATS8600 includes POS devices and they are monitored by a camera system, the *Cash Desk Monitor* monitor panel is used. It pairs cash desk transactions with camera system information.

Cash Desk Monitor monitor can be selected in the *View* menu.

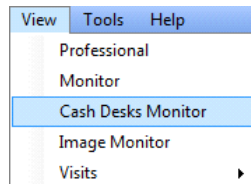


Figure 14-1 panel Cash Desk Monitor

To set up the *Cash Desk Monitor* panel.

1. In the *Devices* tree, create a cash desk and a camera system, which will be used in the next steps. Added devices will include a cash desk, cash desk bus controller and a camera system with at least one camera. Detailed information about devices creation is described [in chapter Adding a device](#).
2. Use the method described [in chapter Connecting a camera to a device](#) , pair the cash desk with a camera that will monitor it.

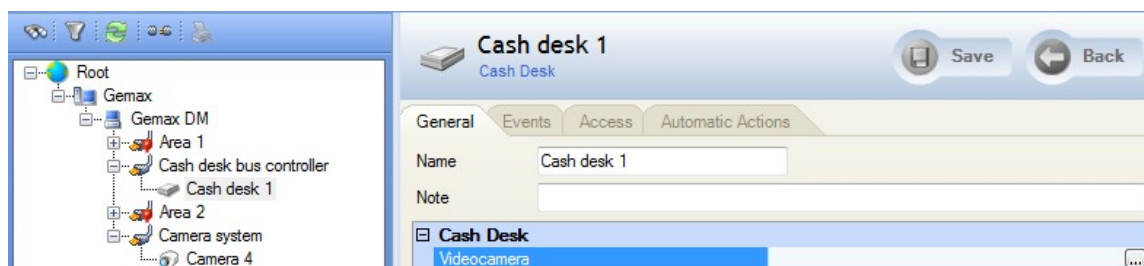


Figure 14-2 Pairing a camera with a cash desk

3. Open *Cash Desk Monitor* from the menu.
4. You can search this panel for the required cash desk and track it. You can look for a cash desk or camera feed from a cash desk using attributes:
 - *Cash desk number* - cash desk ID
 - *Transaction number* - receipt number
 - *Cashier internal number* - personal number of an employee in ATS8600
 - *Article code*

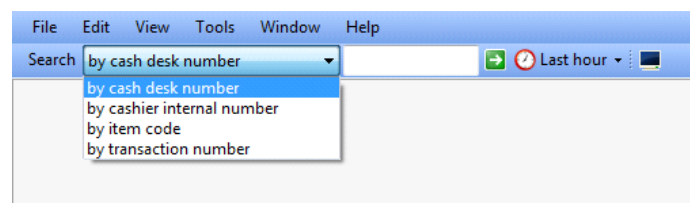


Figure 14-3 Searching a cash desk

5. You can view the following information in the searched cash desk:
 - The left area of the window shows the camera system from the searched cash desk
 - Cash desks transactions - the upper right-hand corner shows the list of cash desks transactions,

- which are gradually added as they are processed by cash desks
- Transaction items - the list of items (articles in one receipt) for the selected transaction.

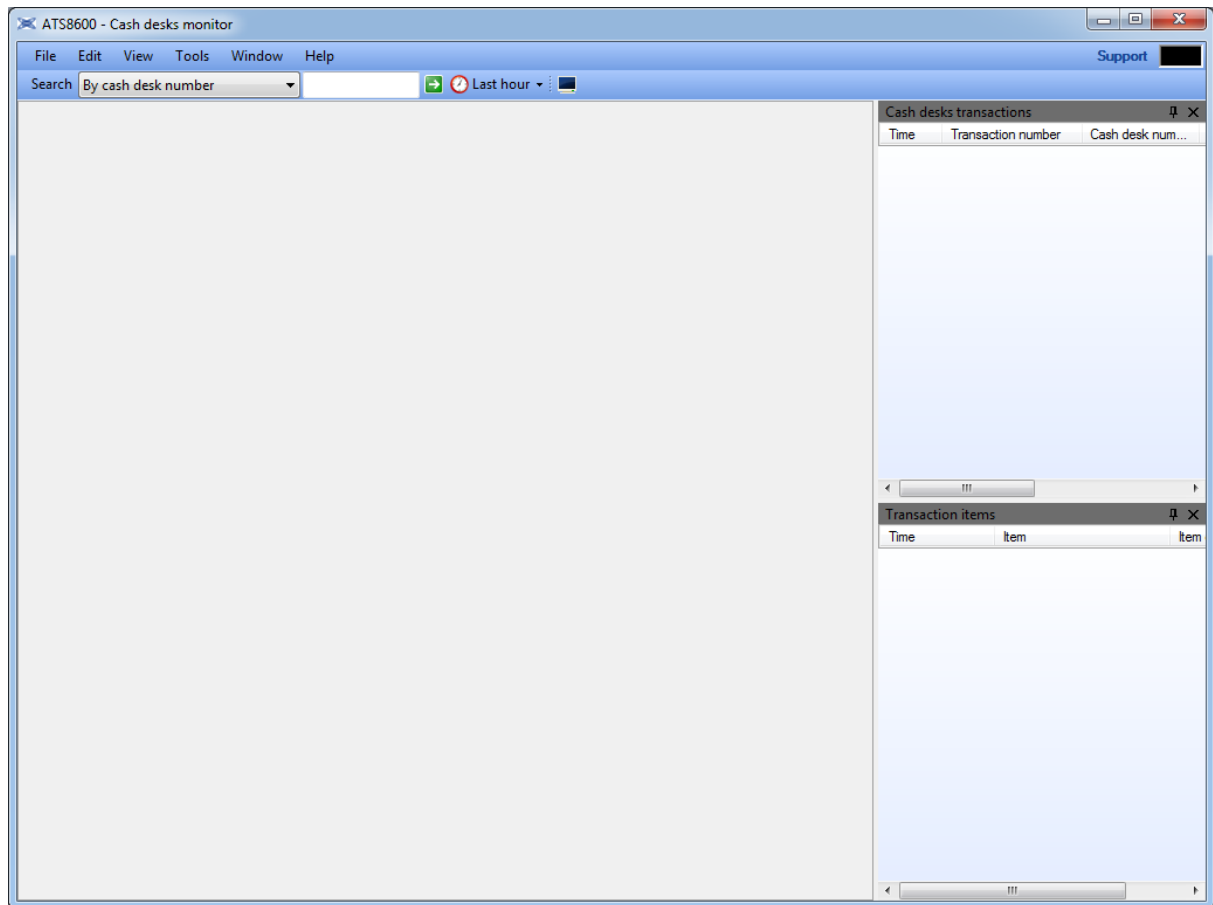


Figure 14-4 Cash Desk Monitor

You can monitor a cash desk online or you can search for a past record according to the available attributes.

In practice, this functionality is used to:

- evaluating complaints - comparing purchased posted items,
- controlling goods loss - checking the number of posted items,
- to check non-posted items.

15 Events

As ATS8600 is a system for monitoring and coordinating persons' access to devices, recording of events is an essential part of the system.

The application enables you to follow all activities within the system from persons or devices.

The log of all activities can be found in the Events tab in the Navigation panel. Events are recorded automatically in chronological order: the latest event is on top of the list.

15.1 Person related events

Selecting a person in the *Persons* tree and click the *Events* tab will display controls in the right corner of the screen providing option to select select events related to that person using an assigned credential or the use of the application. Only those events that the person is authorized to view are displayed. Every event record includes information on the device from which the event originated, the event type and the exact date and time.

Events of individual persons can be filtered. There are three default event filters available:

- *Access events* - all events that relate to the use of the assigned credentials like access denied or access granted.
- *Activities on devices* - all events caused by the selected persons using the application on devices (like commands issued).
- *All activities* - all activities performed by the selected persons.

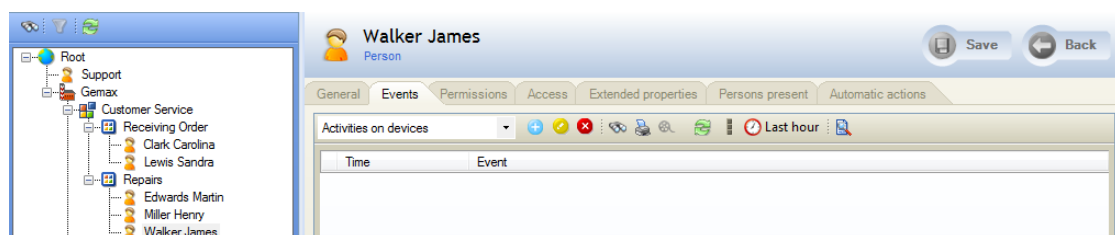


Figure 15-1 Selecting the event tab

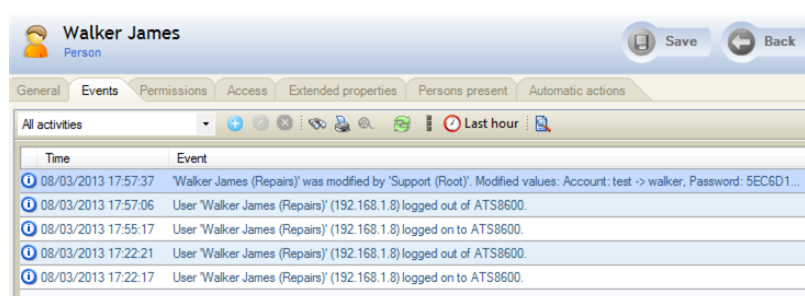


Figure 15-2 Displaying events

If the selected node for which events are displayed has children, then using  you can display events from the parent node and all children of this node (e.g., a department and all employee) by clicking the **With children On** button. Click **Refresh** to update the list. In case of a large number of records you can use the displayed scrollbar to scroll the list and view events displayed below. When reaching the last record, more records will be loaded. The end of the list will be reached when it is no longer possible to move the scrollbar, i.e., it will be at the bottom of the list.

An event can have one of the following priority levels, which is indicated by the icon at the beginning of an event:

-  - information
-  - status change
-  - warning
-  - error
-  - alarm

You can use the  button to print the list of events.

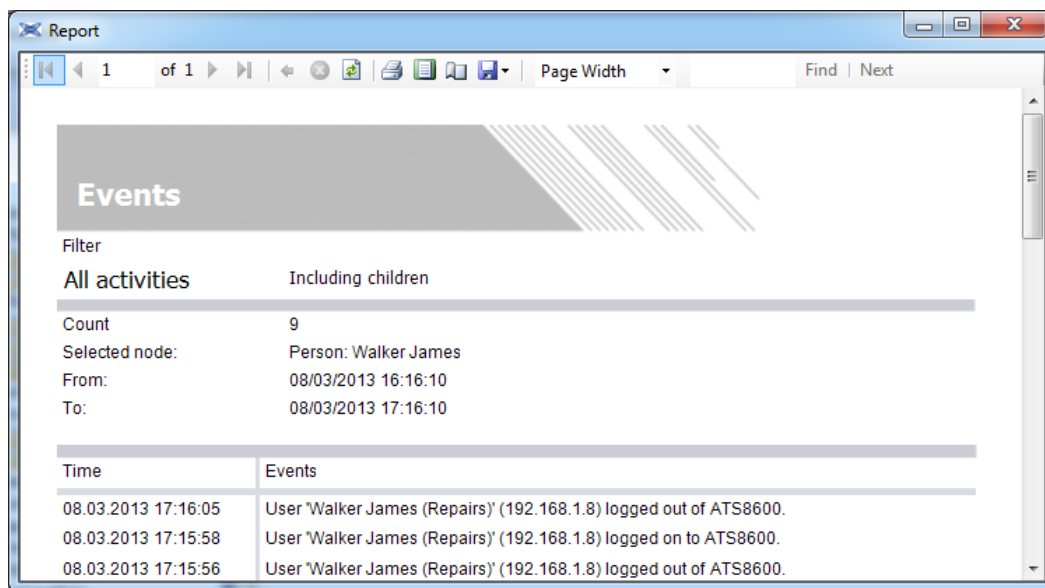


Figure 15-3 Printing events

By clicking Time , it is possible to set a filter based on time and date. Only activities performed within the entered time and date range will be displayed. For the *Persons* and *Devices* trees the default value is one hour. If you wish to display events within another time period, enter the value required, click **OK** and then **Refresh**. The entered time period is valid only for this view. These settings will not be stored.

When starting the application the default events viewing setting will be reset to 1 hour again. The default format of date and time in the entire ATS8600 application is according to the date and time formats set in Windows.

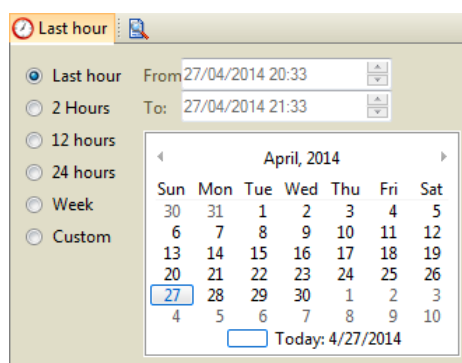


Figure 15-4 Setting a time filter

After pressing  in Events, you can display or hide a window containing notes stored with the selected event.

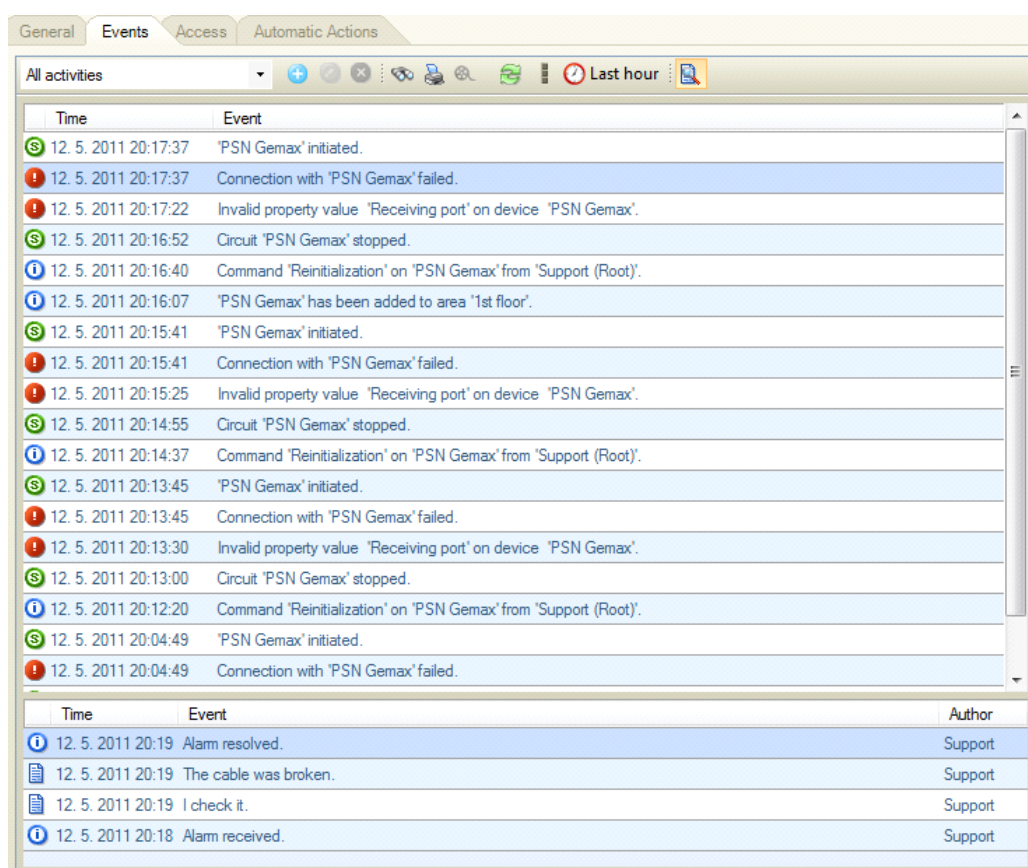


Figure 15-5 Displaying a window with notes stored with the selected event

15.2 Device related events

In the *Devices* tree, select a device and then click the *Events* tab; a list of all events related to this device will be displayed on the right-hand side of the screen. Every event record includes additional information like the person related or the changes applied in the ATS8600 settings of the device. Only events from devices for which the user was granted access will be displayed.

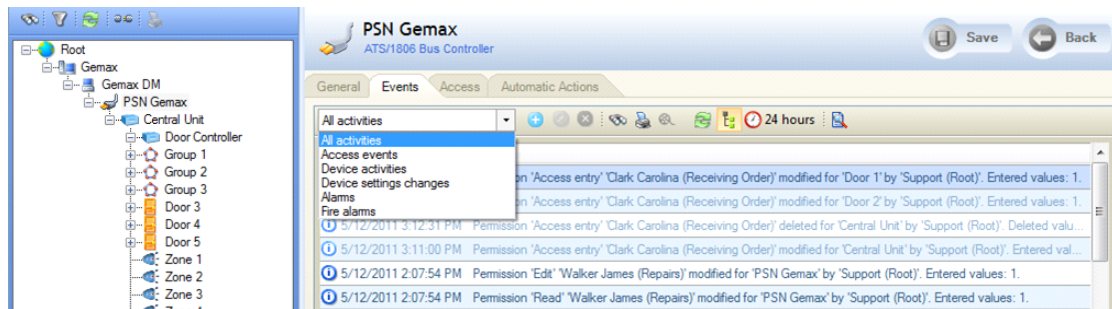


Figure 15-6 Events from a device

Events of individual devices can be filtered. There are six default event filters available:

- *All activities* - all activities performed related to the devices.
- *Access events* - list of all access events on the selected devices.
- *Device activities* - all events related to the selected devices using the application (like commands issued).
- *Device settings changes* - all events related to creation or modification of settings in ATS8600 on the devices.
- *Alarms* - list of alarm events on devices.
- *Fire alarms* - list of fire-type alarm incidents on devices.

By clicking Time , it is possible to set a filter based on time and date. Only activities performed within the entered time and date range will be displayed ([see chapter Person related events](#)).

15.3 Viewing events using regions

The system provides the option to view events based on regions in the parent region and in all sub-regions, i.e., events related to regions like the use of credentials by persons on devices or commands issued through the application or events from devices in the regions. If you wish to view all events that took place in the *Office 101* region, for example, select this sub-region and next the *Events* tab in the right-hand side of the screen.

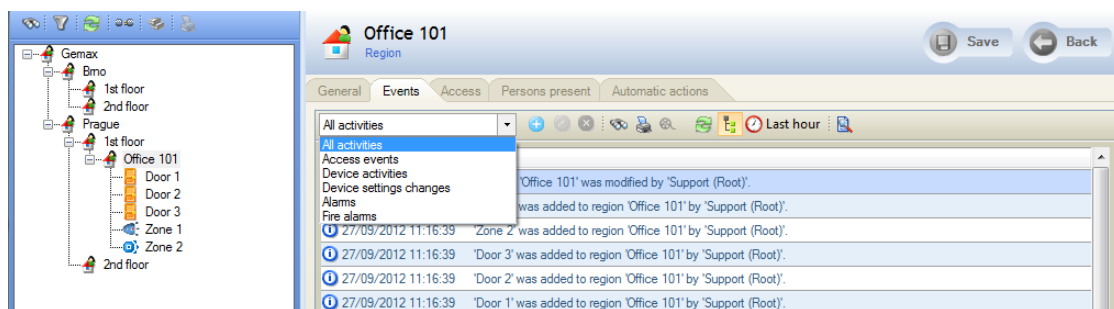


Figure 15-7 Events in the selected region

To view the device events in the selected region and sub-regions, select the option to include children of this region by clicking the children function.

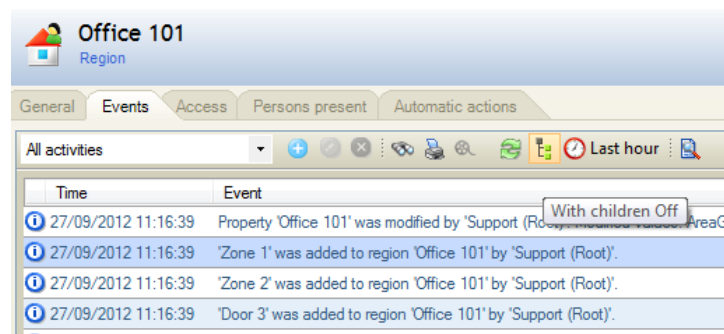


Figure 15-8 Show also children

Events can be filtered. There are six default event filters available:

- *All activities* - all activities performed related to the region (and its subregions, if the **With children On** function is activated).
- *Access events* - list of all access events in the selected region.
- *Device activities* - all events related to devices in thus using the application (like commands issued) if the **With children On** function is activated.
- *Device settings changes* - all events related to creation of modification of settings in ATS8600 on the devices.
- *Alarms* - list of alarm events in the region.
- *Fire alarms* - list of fire-type alarm incidents in the region.

By clicking Time , it is possible to set a filter based on time and date. Only activities performed within the entered time and date range will be displayed

15.3.1 Searching for video records with events

ATS8600 Integrated Security Management System, including a video camera system, enables the user to search for stored video recording based on the time-stamp of an event. It is used mainly in cases when an unexpected event occurs and video footage from a (linked) camera may support in understanding and resolving the reason for the event.

In the *Regions* tree, find the events list of the related device. If there is a video camera located in the region, you can select the recording within the required time range when the event occurred.

Note:

The *Events* tab can also be found in the *Replications* and *Visitors management* modules.

15.4 Printing reports

Event printing is available in all *Events* tabs (*Persons*, *Devices* and *Regions*) . Printing of various lists can be helpful when creating reports. You can print the reports created or save them in Microsoft Excel (.xls) format and utilise the collected data in various ways.

Events	
Filter	
All activities	Including children
Count	47
Selected node:	Region: Gemax
From:	26/09/2012 11:21:56
To:	27/09/2012 12:21:59
Time	Events
27.09.2012 12:17:21	Property 'Prague' was modified by 'Support (Root)'. Modified values: Alarm propagation.
27.09.2012 12:16:42	Property 'Prague' was modified by 'Support (Root)'. Modified values: Alarm propagation.
27.09.2012 12:16:42	Property '1st floor' was modified by 'Support (Root)'. Modified values: Alarm propagation.
27.09.2012 12:16:42	Property 'Office 101' was modified by 'Support (Root)'. Modified values: Alarm propagation.

Figure 15-9 Resulting print report

Note:

A printer must be added to the computer and configured.

To save a print report as a Microsoft Excel (.xls) file, click  and choose the appropriate file format.

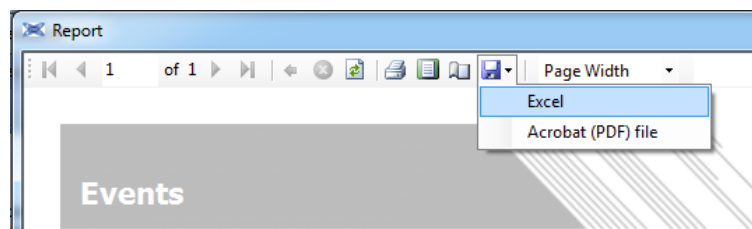


Figure 15-10 Saving a report

You can print a report by clicking  and entering the printing parameters.

15.5 Event monitoring

The system monitors and records events and the date and time when the event happened, according to the time set in the user environment of the person logged in the application.

15.5.1 Access for authorised persons

To gain access a person badges the card in front of the reader, enters a valid PIN code or a combination of both of these; a signal will sound to indicate that the card was read and accepted. The access granted event record will be shown in the person's activities list and in the list of activities of the device that registered the access.

15.5.2 Access denied

An access attempt at a device by an unauthorised person is referred to as invalid access attempt. This occurs if a person badges an invalid card in front of a device. A signal will sound to indicate that the card was not accepted. Invalid means that the credential used to identify the person could not identify the person or the person is known but is not allowed access through the device.

An Access denied record will be shown in the *Events* tab of the *Devices* tree. The respective card number is displayed in brackets in the details of the event.

15.5.3 Using Request To Exit button

Pressing the Request To Exit button will allow the person to leave (if no credential on exit is needed). Overview on the exit button usage can be viewed using the device *Exit button* of the *Events* tab of the device that registered the activity. The record includes the message *Exit button pushed*.

15.5.4 Eliminated Door

After a door has been broken down or opened without a proper credential, the *Eliminated door warning* will appear in the *Events* tab of the respective *Devices* tree.

15.5.5 Door open too long

Person identifies himself (e.g., badges the access card in front of a reader); signal can be heard - identification was successful. Person holds the door open during a period longer then allowed in the properties of the device.

The *Door open too long* warning will appear in the *Events* tab of the *Door* device.

15.5.6 Remote opening of a Door

The door can be opened remotely by an application user by right-clicking the respective *Door* in the *Devices* tree and selecting command *Open* in the pop-up menu.

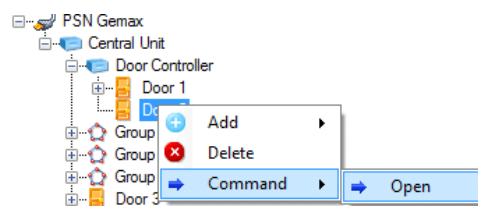


Figure 15-11 Remote opening of a door

The door will open and the *Remote Door Open* message will be displayed in the *Events* tab of the respective *Door* device in the *Devices* tree.

A related message will appear in the *Events* tab of the *Persons* tree of the person who issued the command.

15.5.7 User activities

User activities performed in ATS8600 and in line with the user's application permissions are also recorded as events and include mainly the following: modification of settings, deleting of objects, renaming, etc. These events can be viewed in the *Events* tab of the respective device or person.

Events on devices can also be monitored in the *Events* tab of the respective device.

15.6 Event filtering

Event filtering is used to select events according to requirements of the user, based on the filtering conditions.

For each tab (*Persons*, *Devices*, *Regions*), the user can create his/her own event filter, edit it or delete it by using the **Add**, **Edit** and **Delete** buttons. This concerns the predefined filters as well.

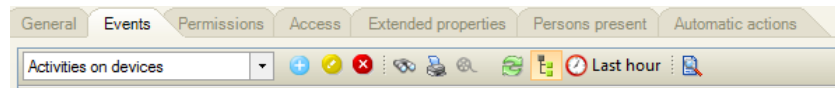


Figure 15-12 Add, Edit and Delete icons

-  - creates a new event filter
-  - modifies a predefined or custom event filter
-  - deletes a predefined or custom event filter

Warning:

The following predefined filters cannot be edited, nor deleted:

- *All activities* (in *Persons*, *Devices* and *Regions* trees)
- *Card activities* (in *Persons* tree in *Credentials* tab)
- *Automatic actions activities* (in *Automatic actions* tab, *History* window)

15.6.1 How to Create an Event Filter

After clicking , the user can select the filtering conditions that will be used as an event filter.

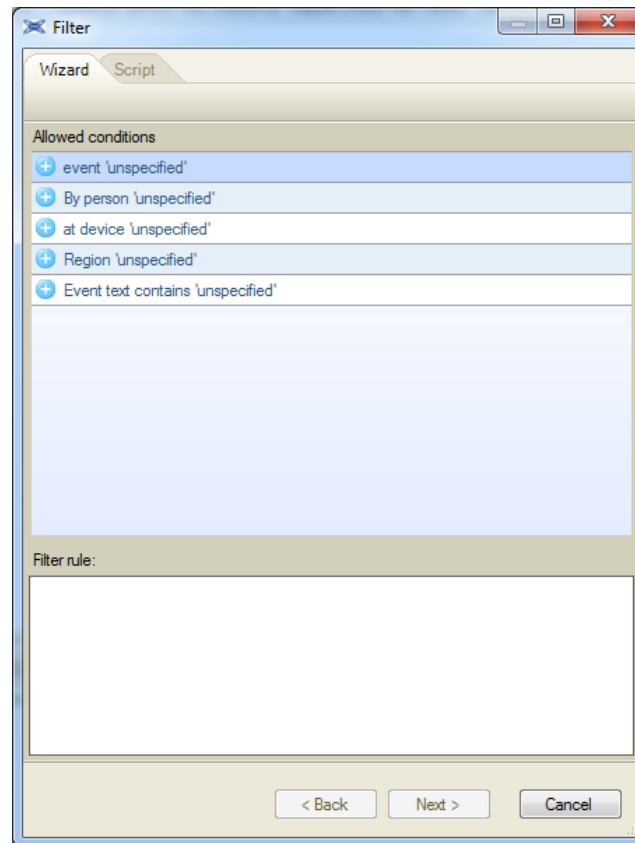


Figure 15-13 Creating a custom event filter

The user can select the following filtering conditions:

- Event - event selection for filtering
- Person - choose a person related to the monitored event
- Device - device selection for which the event monitoring should be performed
- Region - region selection, where the event monitoring should take place
- Event text - option to select a text string that contains the event

15.6.2 Example of creating a new event filter

We will demonstrate the principle of creating a new event filter in the *Persons* tree, where we create a new filter: User ATS8600 login and logout monitoring.

Click the Event from the enabled windows menu and click **Unspecified** to create a filter condition.

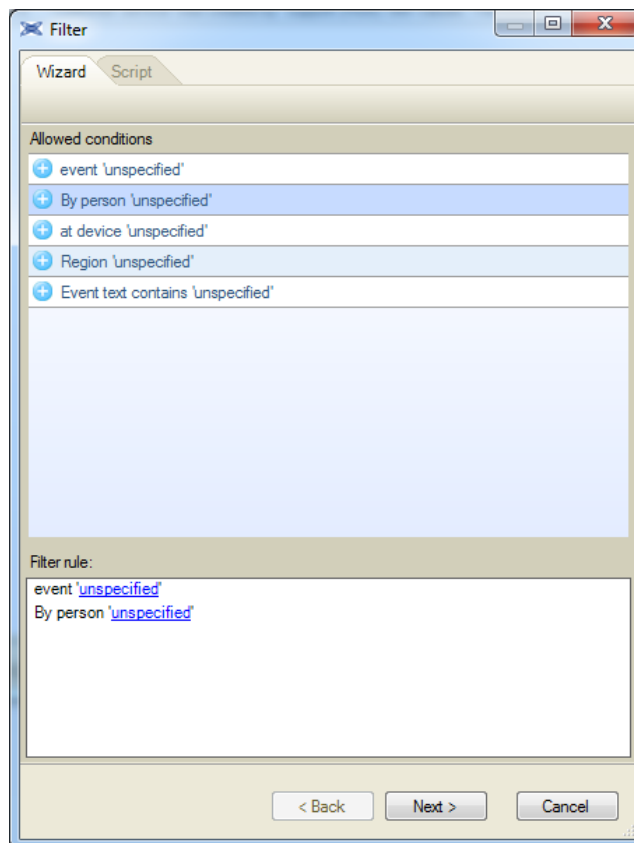


Figure 15-14 Filtering conditions

Note:

To delete a filter condition, right-click the condition and click **Delete**.

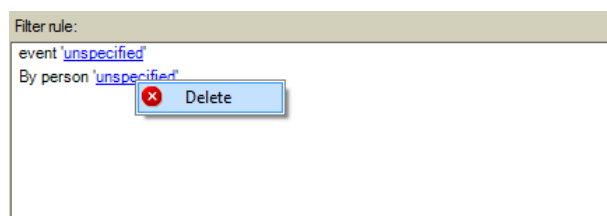


Figure 15-15 Deleting a filtering condition

Click **Unspecified** to display a list of events available in the application. The event list gradually appears in the text field while being filtered. Select **"Login"** and then **"Logout"** from ATS8600.

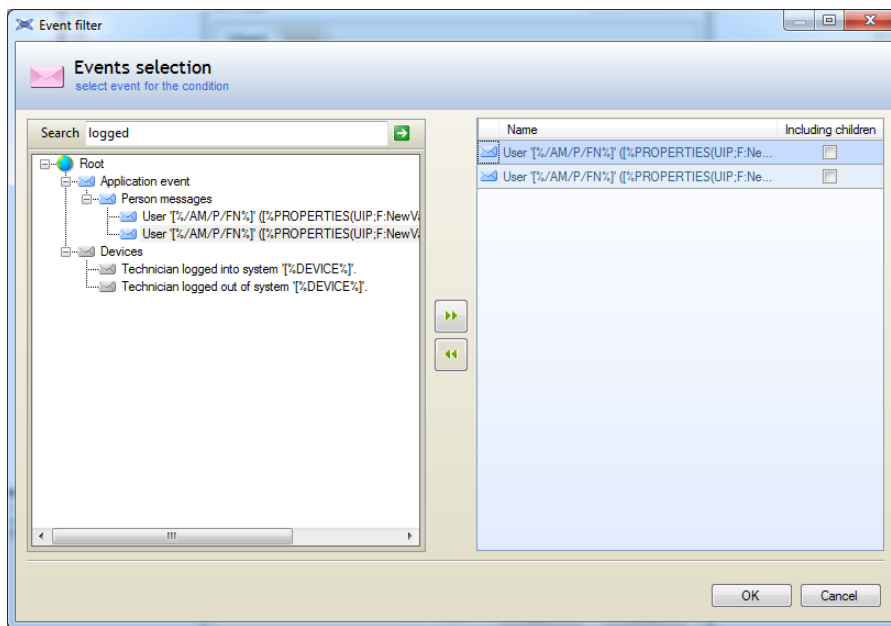


Figure 15-16 Selecting an event

From the enabled filter conditions, select the person to be filtered for the event.
Click **Unspecified** and select the person from the tree, e.g. *Carolina Clark*.

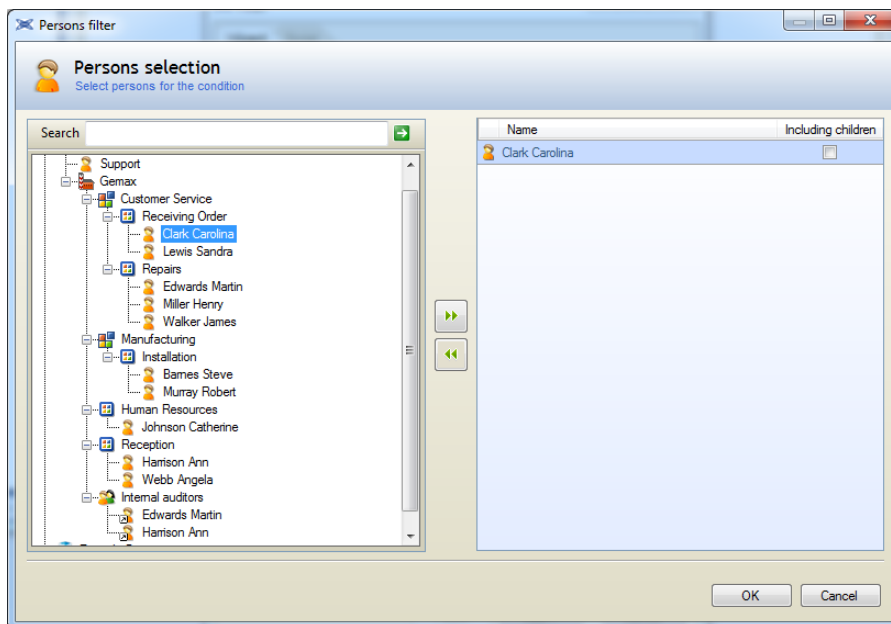


Figure 15-17 Selecting a person

After making the selection, click **Next** in the filtering condition.



Figure 15-18 Defining filtering conditions

Enter a descriptive name of the filter, such as: *"Login and logout of Clark"*

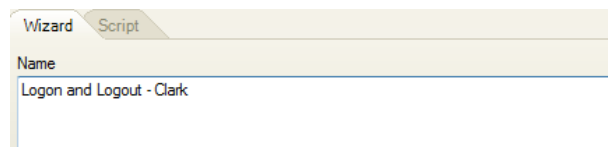


Figure 15-19 Naming the filter

After finishing the wizard, the selected person will have the newly created filter appear next to the predefined filters in the filters list.

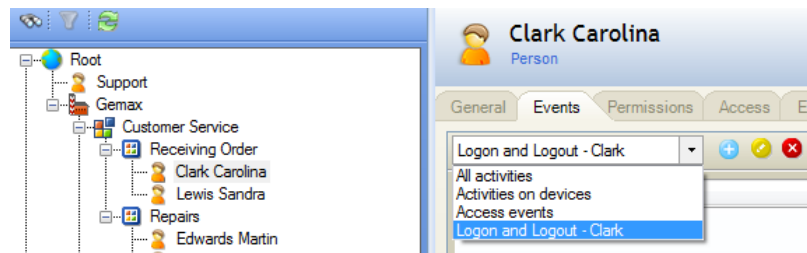


Figure 15-20 Newly created event filter

After login and logout of Caroline Clark into ATS8600, a message appears within the events:

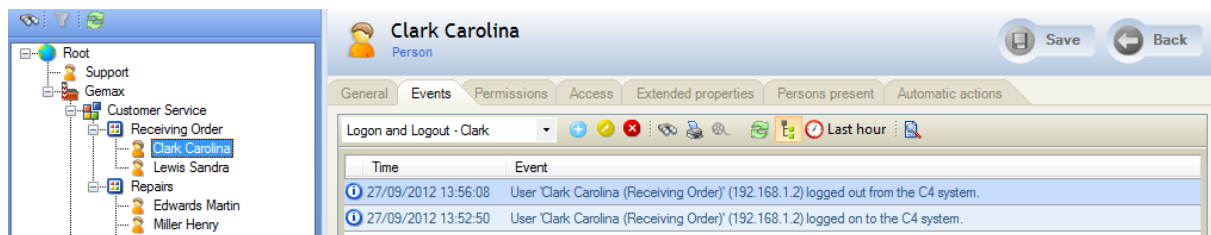


Figure 15-21 Displaying the login and logout of Caroline Clark

If the application administrator wants to prohibit certain persons from displaying the filter, he/she needs to set permissions to individual event filters ([see chapter Types of permission](#)).

16 Automatic actions

Automatic actions allow the definition of logical relations between individual devices managed in ATS8600 application. At the same time they assist in automation of processes.

Example:

An automatic action is when the entered area is disarmed after swiping a card by its holder. The purpose of that automatic action is that the system immediately recognises the card holder and does not require entering any disarm code.

Automatic actions also have many advanced purposes, e.g., automatic setting of air-conditioning if there are more than 10 people in a room.

Administrating automatic actions means:

1. selecting the event types to initiate automatic actions;
2. selecting the devices to monitor these events;
3. set a person to whom a notification should be sent or to set the execution of any command.

Automatic actions consist of two main parts:

1. set of conditions, on the basis of which the automatic action itself will subsequently be performed
 - these conditions can be defined by a set of events that arose in ATS8600
 - they can be defined from individual statuses of devices
 - they can be based on the fact that a user issued a command inATS8600
1. the form in which the automatic action will be performed:
 - email, SMS or executing a command that can be performed by a person on the devices inATS8600

To predefine automatic actions, select *Automatic actions* from the *Tools* menu.

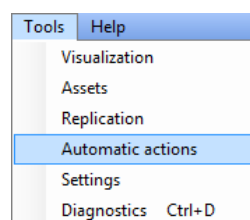


Figure 16-1 Menu selection Automatic actions

The automatic actions panel is displayed. Here automatic actions are managed. Click  to select the function for creating a new automatic action.

This panel consists of two main parts:

- the upper part displays the list of set automatic actions
- the second part is the *History* window, which can be pinned on top or closed

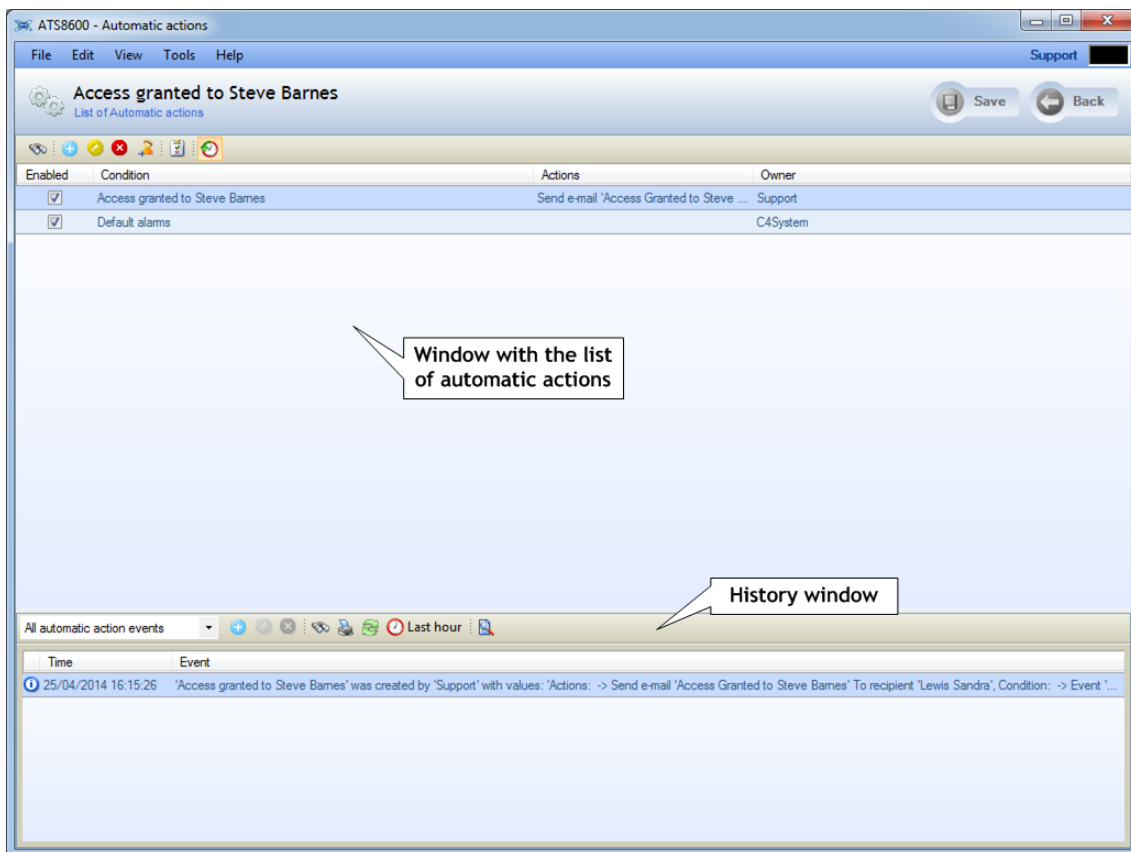


Figure 16-2 Automatic actions panel

Warning:

The system contains a predefined automatic action called *Default alarms*, which ensures that event delivery to alarm management. This automatic action cannot be deleted. Only a qualified person should modify it.

16.1 Procedure for setting automatic actions

The first step in defining an automatic action is to select its type. A filter-like list of types of actions opens in a new window.

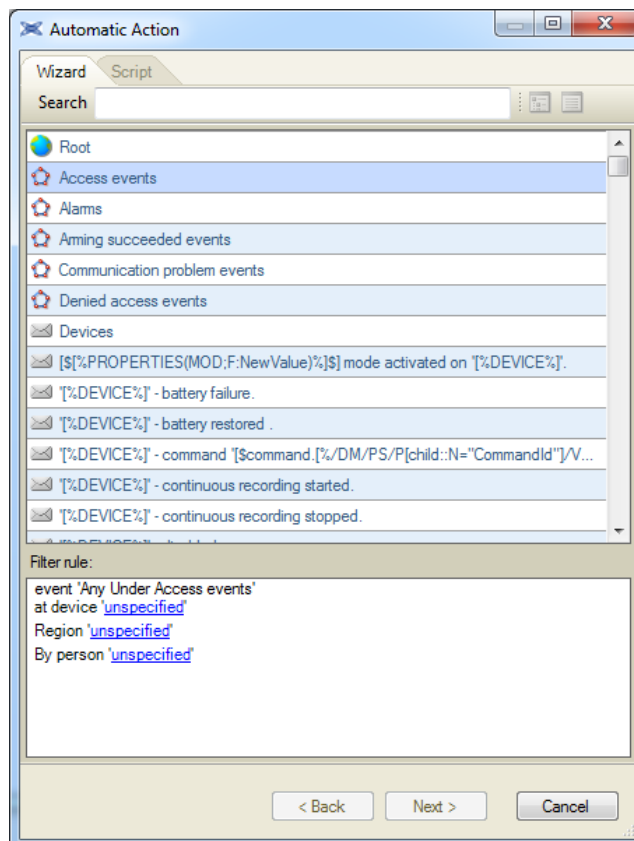


Figure 16-3 Window for creating an automatic action

While writing into the *Search* field, the results are gradually filtered and only the automatic actions containing the searched text in their name are displayed. Select *Access Granted*

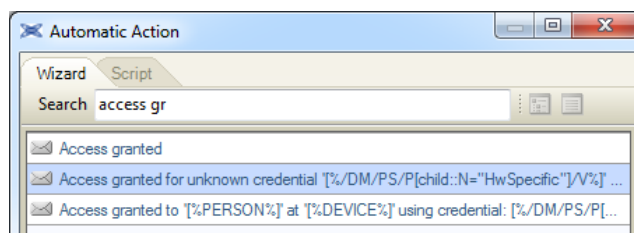


Figure 16-4 Defining the automatic action type

The next step is to select devices for the automatic action type for which these action should be monitored and executed. Click the link for setting devices in the lower part of the window.

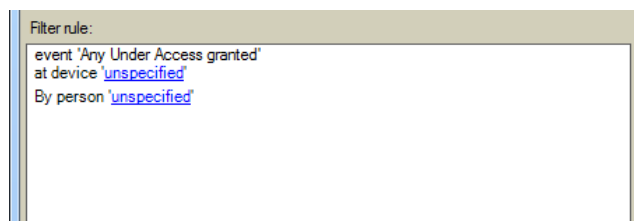


Figure 16-5 Setting the device for automatic action

By clicking the link a window for selecting devices will open.

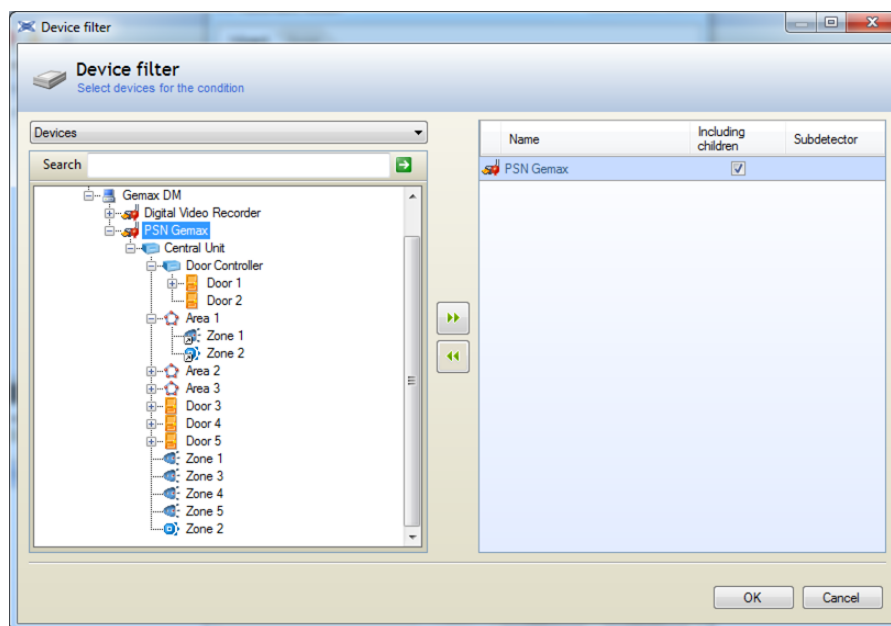


Figure 16-6 Selecting devices for the automatic action

In the *Devices* tree in the open window, find the required device, select it and move to the list on the right side of the window.

Check the With children box to set the automatic actions to apply also to devices that are considered to be children in the hierarchical structure

Click the person setting link in the same window to select persons who will perform automatic actions.

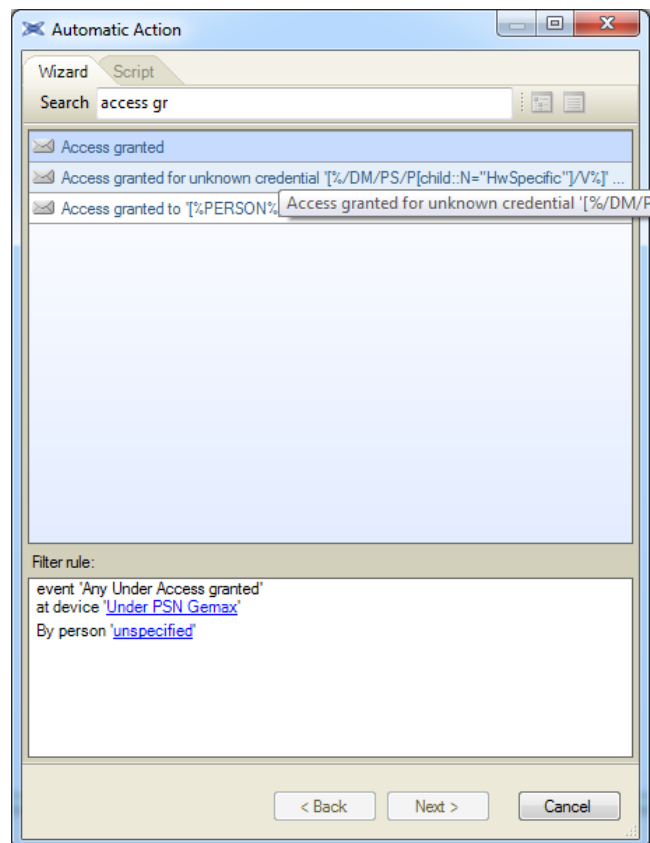


Figure 16-7 Setting a person for an automatic action

A window for selecting persons for the automatic action opens. The system of selecting from the tree is similar to devices.

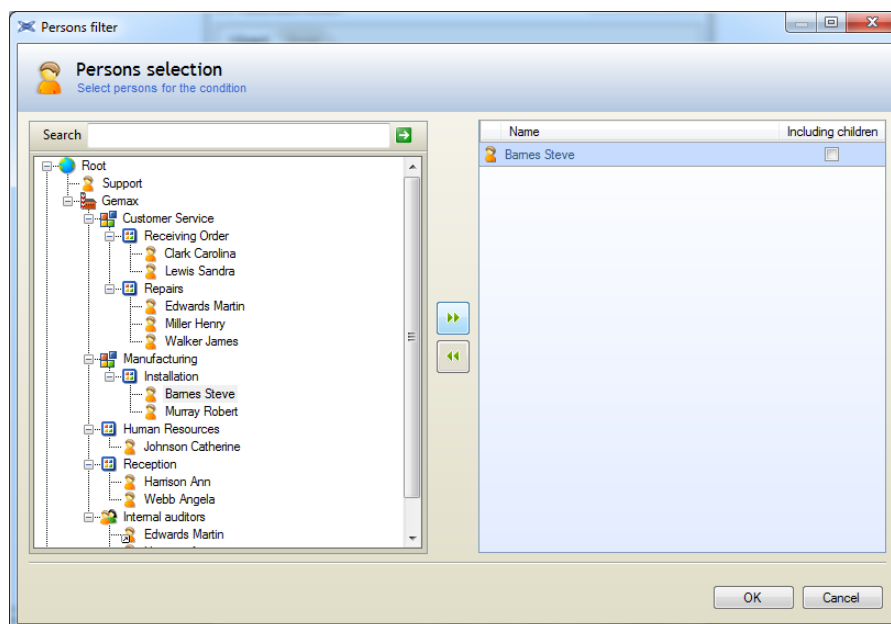


Figure 16-8 Setting a person for an automatic action

Devices and persons for an automatic action are set when the text of the link changes to the respective device, group of devices or persons.
Click **Next** to continue.

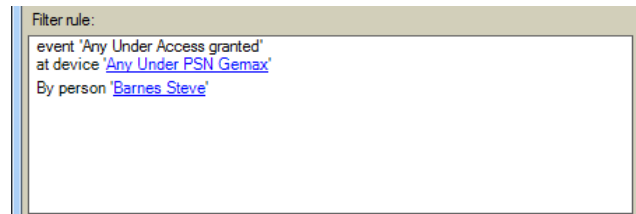


Figure 16-9 Set devices and persons

In the window that opens it is necessary to select the form in which the automatic action should be performed. Following types of actions are available:

- **Send command** - this means that if the selected event "Access Granted" occurs, the system should send a command to execute the event. This command can be defined on the following screen of the wizard.
- **Send e-mail** - setting the recipient and body of the email.
- **Send SMS** - setting the recipient and body of the SMS.
- **Increase/decrease counter** - the user enters the variable name and a value by which the value will be increased/decreased when the event occurs.
- **Start timer** - the user enters a name and value of a variable, which will be used as a starting value for the timer
- **Stop timer** - stops a running timer
- **Set off an alarm** - the event that initiated this action will be evaluated as an alarm in the *Alarm management window*.

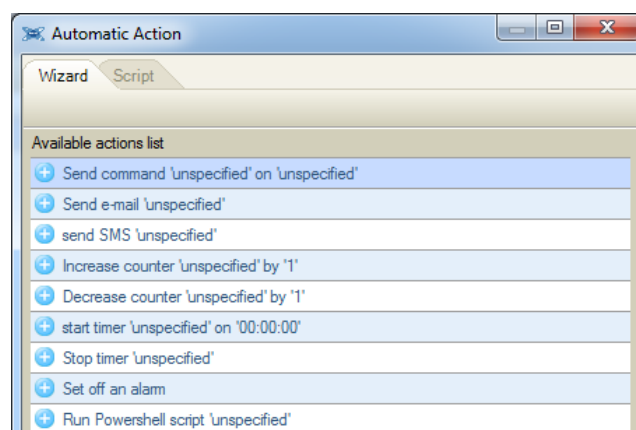


Figure 16-10 Action selection

Double-click the selected item to add a link to the bottom part of the window. The link can be used to set the details of the given automatic action (e.g. to choose an email/SMS recipient or specify a command).

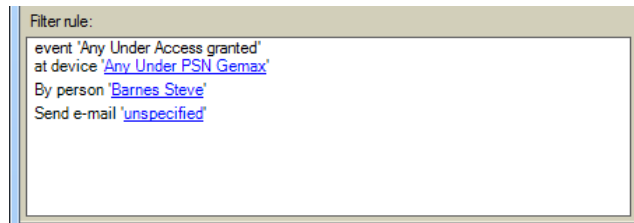


Figure 16-11 Setting an email recipient

In the newly opened window, select a person or several persons from the tree and add them to the list in the right-hand side of the window. These persons will be the recipients of the email for the selected automatic actions. In the Text box, enter the text of the email that will be sent to the selected persons if the automatic action *Access Granted* occurs. If you want to send an SMS message, a similar window will open.

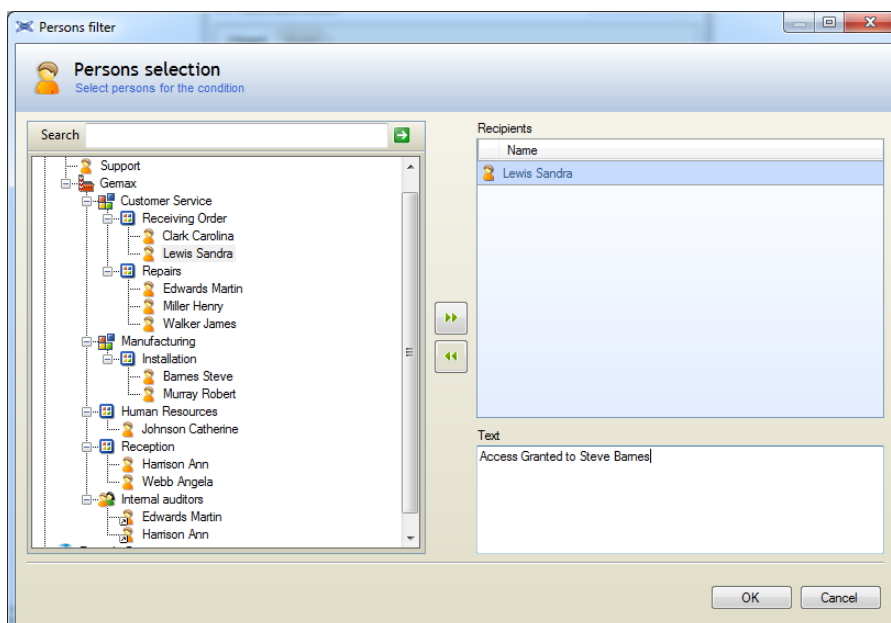


Figure 16-12 Setting the recipient of the email or SMS

Click **OK** to confirm the selection and save settings. The automatic action conditions are at the bottom of the window.

So far, we have set the system such that if it records *Access Granted* for the *multiple devices* set by *Steve Barnes*, it should send an email to *Sandra Lewis*.

Tip:

If the text field is left blank, the recipient receives a text of the event that caused the automatic action.

Warning:

The person selected as an automatic action email recipient must have his/her e-mail address entered in the *Contact* tab in ATS8600.

The person selected as an automatic action SMS message recipient must have his/her phone number entered in the *Contact* tab in ATS8600.

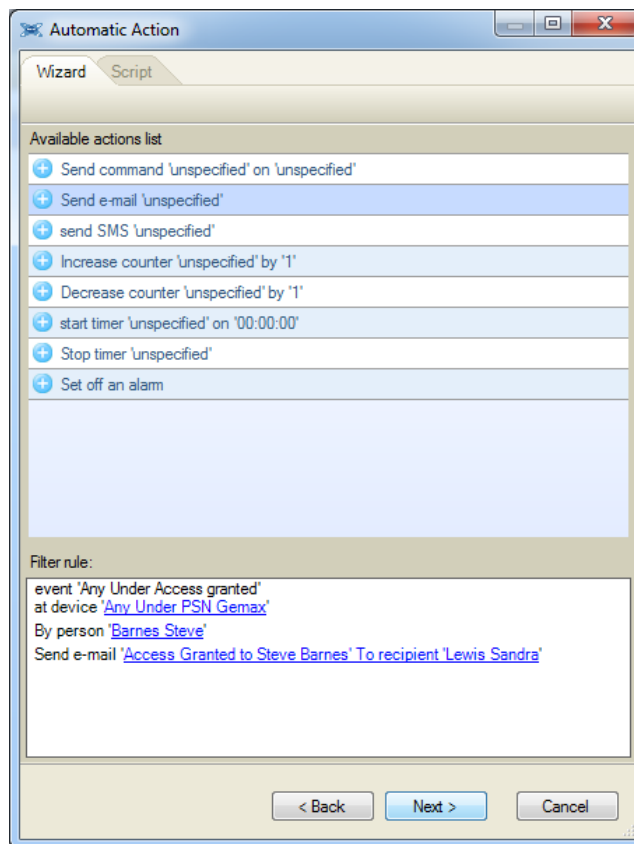


Figure 16-13 Automatic action setting

To set a command for the automatic action, double-click the **Send command** at the top of the window to add a link for setting the command to the bottom of the window.

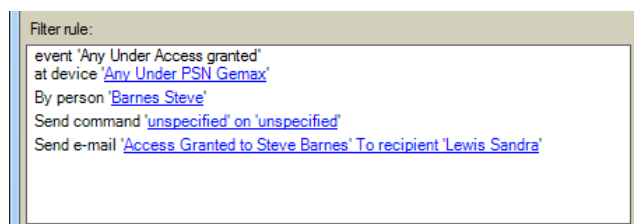


Figure 16-14 Link for setting a command

Click the link to open a command setting window.

An example of an automatic action executed in the form of a command is when a room automatically disarms when a specific person enters it.

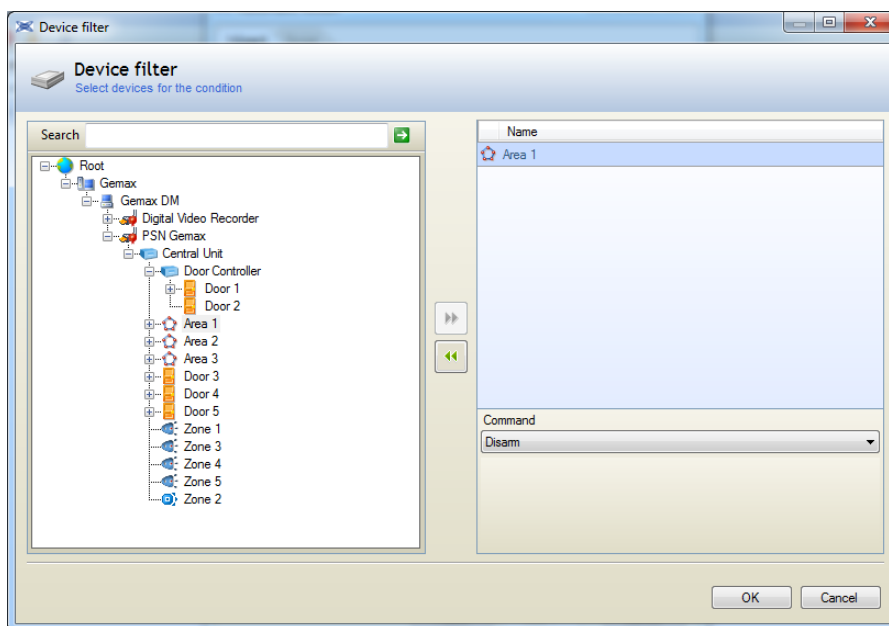


Figure 16-15 Setting an automatic action command



Figure 16-16 Parameters of an automatic action

If you do not wish to set more conditions for an automatic action, click **Next** to confirm the setting. In the next step the system will prompt you for a custom name of that automatic action. Enter the name. If you do not name the automatic action and the *Name* field remains blank, the name will be the condition.

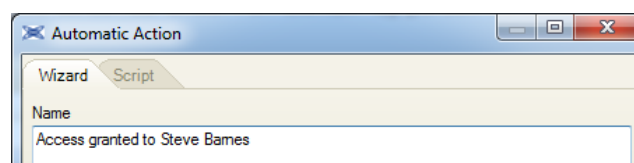


Figure 16-17 Name of an automatic action

After setting an automatic action, a record on that action will be added to the list in the *Automatic actions* panel and after one minute this action will start working.

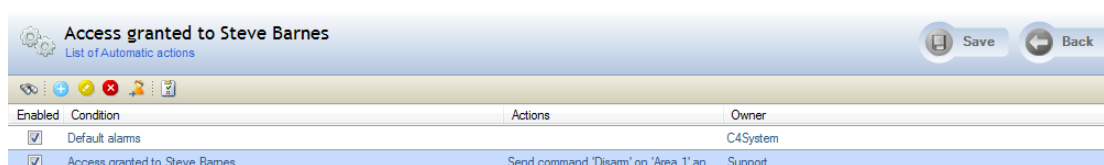


Figure 16-18 Automatic action setting

16.1.1 Automatic action owner

Each automatic action has an owner - the creator of the action. The action is executed in the context of the user who created and set this action and in the context of access rights set in the entire ATS8600 Integrated Security Management System. An owner can therefore set automatic actions only to those objects to which he/she has access rights. Similarly, an automatic action recipient can be notified only of those objects to which he/she has access rights.

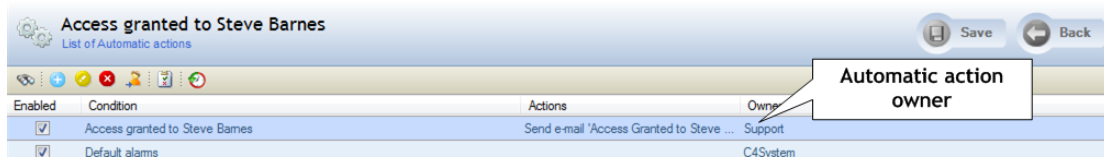


Figure 16-19 Owner of an automatic action

If an automatic action is set for a user and that user is later deleted from the system, the action will be displayed as invalid and greyed out.

However, an invalid automatic action will not be deleted from the system, which means it can be assigned to a new owner using the **Take Ownership** function.

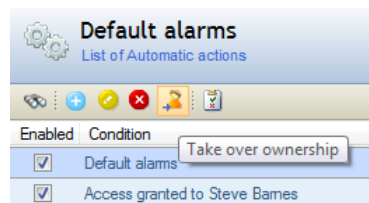


Figure 16-20 Taking ownership

16.1.2 Test an automatic action

An automatic action test uses a simulation of fulfilling the defined conditions of the action without having to wait for the action conditions to actually be met (e.g., actual badging the card in front of a reader).

In case something incorrect has been set for the action, this test will reveal the mistake and it can be corrected before it actually occurs.

Use **Test** to check links between individual conditions of multiple automatic actions to each other (looping), because the system does not check it when automatic actions are set.

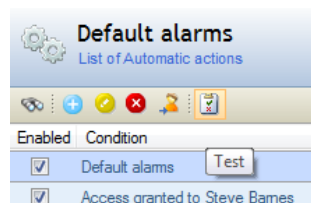


Figure 16-21 Test function

16.1.3 Automatic action script

Each automatic action can be additionally modified by editing its script directly. To edit an action click .

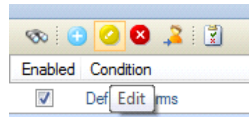


Figure 16-22 Edit automatic action

Selecting this function will open the *Automatic Action* window. Click the *Script* tab and then click **Edit script manually**.

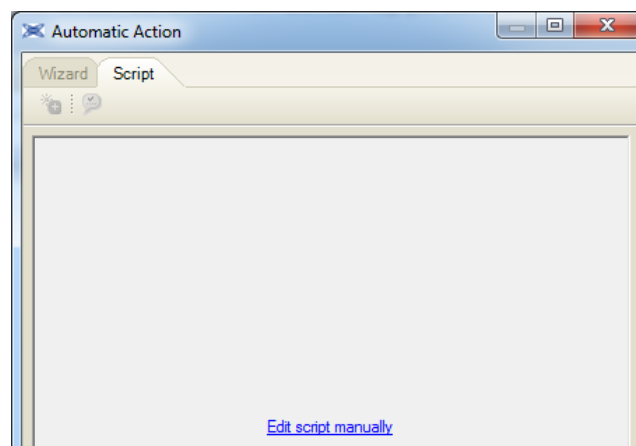


Figure 16-23 Script tab

The system will ask whether you really want to modify the automatic action manually, because no further modification through the wizard will be possible.

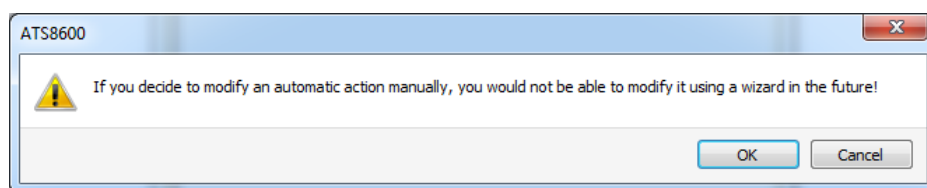


Figure 16-24 Confirming script modification

Once confirmed, the automatic action script will open and can be edited manually.

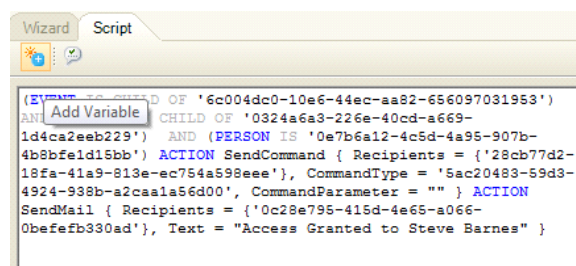


Figure 16-25 Automatic action script: add variable

The **Add variable** function makes it possible to additionally add an object into an automatic action.

By clicking  opens a window, where you can choose a variable of a selected object that you wish to add to the script.

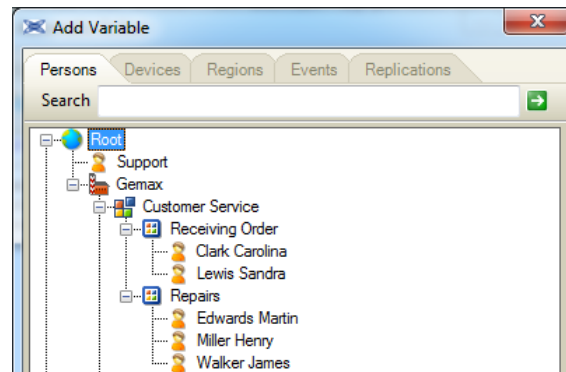


Figure 16-26 Selecting a variable

The function for checking the syntax of the language will be available after the script modification.

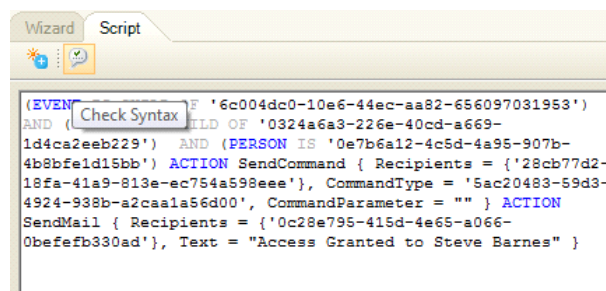


Figure 16-27 Check syntax

In case of a syntax error the system will display an error message.

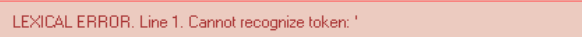


Figure 16-28 Syntax error in the script

Warning:

Editing the script requires a skilled and trained administrator; please request one from the system vendor.

16.1.4 View on the object automatic action

In the *Professional* panel, the relationship of a person or device to the automatic actions being set are shown in the *Automatic actions* tab.

This means that if any person is related to any action, it will be displayed in that tab.

As per the previous settings [in chapter Procedure for setting automatic actions](#), if Steve Barnes is selected, the *Automatic actions* tab shows the actions related to that person.

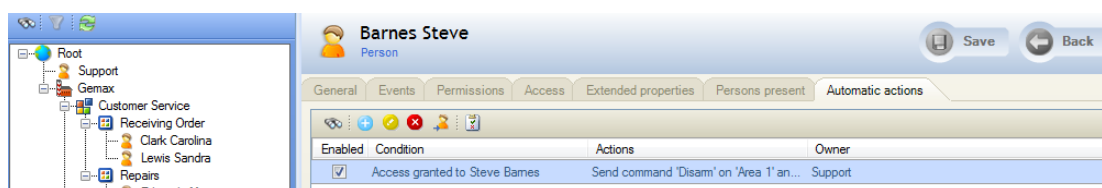


Figure 16-29 Automatic actions tab

16.1.5 Running Powershell Script

Automatic actions allow to run any Powershell script, which ensures an interaction between ATS8600 and other systems.

The script must be saved in the *Scripts* folder, which must be created in the installation folder on ATS8600.

When a Powershell script is called in the Automatic actions wizard, the entire filename including the extension must be entered.

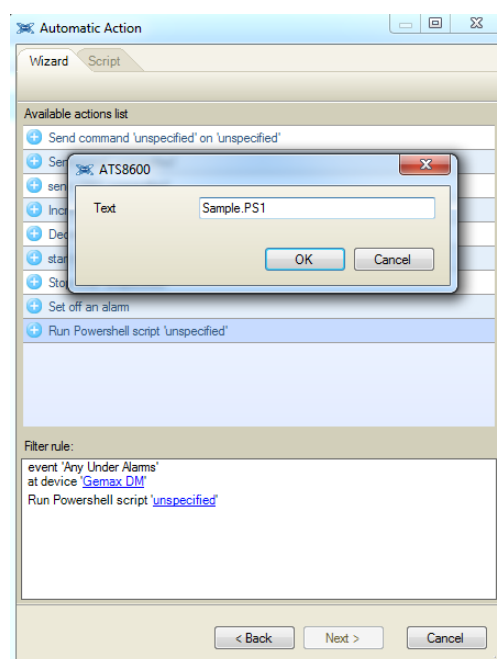


Figure 16-30 Calling a Powershell script

In addition to standard commands, Powershell scripts can include the following syntax of ATS8600.

Method	Description
\$c4.CounterIncrement("counterName", [int] STEP)	Increase the counter "counterName" by the value STEP
\$c4.CounterDecrement("counterName", [int] STEP)	Decrease the counter "counterName" by the value STEP
\$c4.SendCommand([GUID]commandType, [IHandle]destination, [string]parameter)	Send the "commandType" command to the "destination" device with the "parameter" parameter
\$c4.StartTimer([string]name, [TimeSpan]	Start a timer "name" from the value "after"

after)	Example of starting a timer that expires in 1 hour and 25 minutes: \$timespan = new-timespan -hour 1 -minute 25 \$c4.StartTimer("timer1", \$timespan)
\$c4.StopTimer([string]name)	Stop the timer "name"
\$c4.SendSms([IHandle] recipient, [string] text)	Send an SMS to "recipient" with the content "text"
\$c4.SendEmail([IHandle] recipient, [string] text)	Send an e-mail message to "recipient" with the content "text"
\$c4.GetDeviceId([Guid]"someguid")	Get the value "DeviceID" from the unique identifier of the device
Parameter	Description
\$eventId	unique identifier of the event type
\$devices	enumeration of all devices related to the event that initiated the given automatic action
\$persons	enumeration of all persons related to the event that initiated the given automatic action
\$properties	enumeration of all properties of the event

16.2 Setting parameters

To send emails and SMS messages by the ATS8600 server, the e-mail server and SMS gateway parameters must be defined in order to provide notification of selected events.

16.2.1 Email server

Setting of email server parameters is determined by settings of the particular email server; in other words, it is necessary to enter information required by the given server.

Select *Tools - Settings - System settings - Mail server* tab in the main application menu and enter the necessary details.

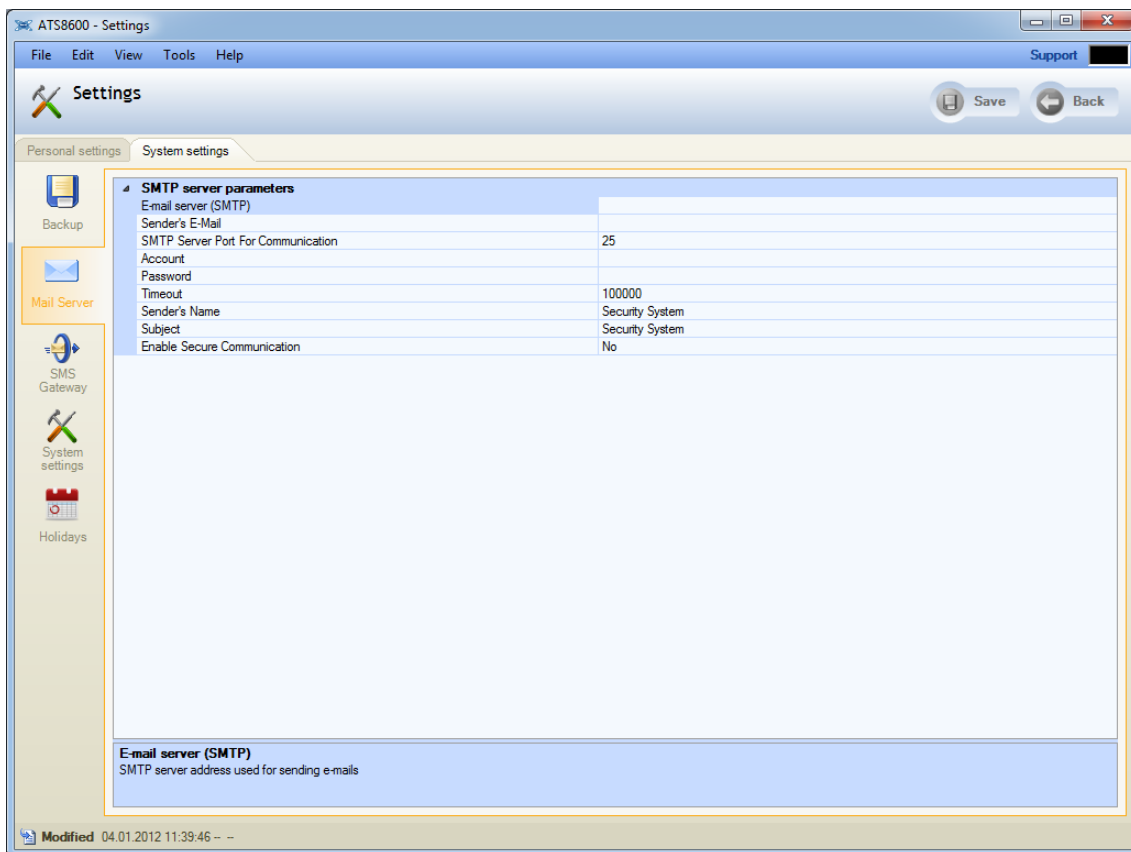


Figure 16-31 Email server parameters

Warning:

For more information on these parameter settings, consult your email server administrator.

Warning:

After setting the email server parameters, restart the *Message Broker* service.

16.2.2 SMS gateway

Select *Tools - Settings - System settings - SMS Gateway* tab in the main application menu and enter the details required by the operator.

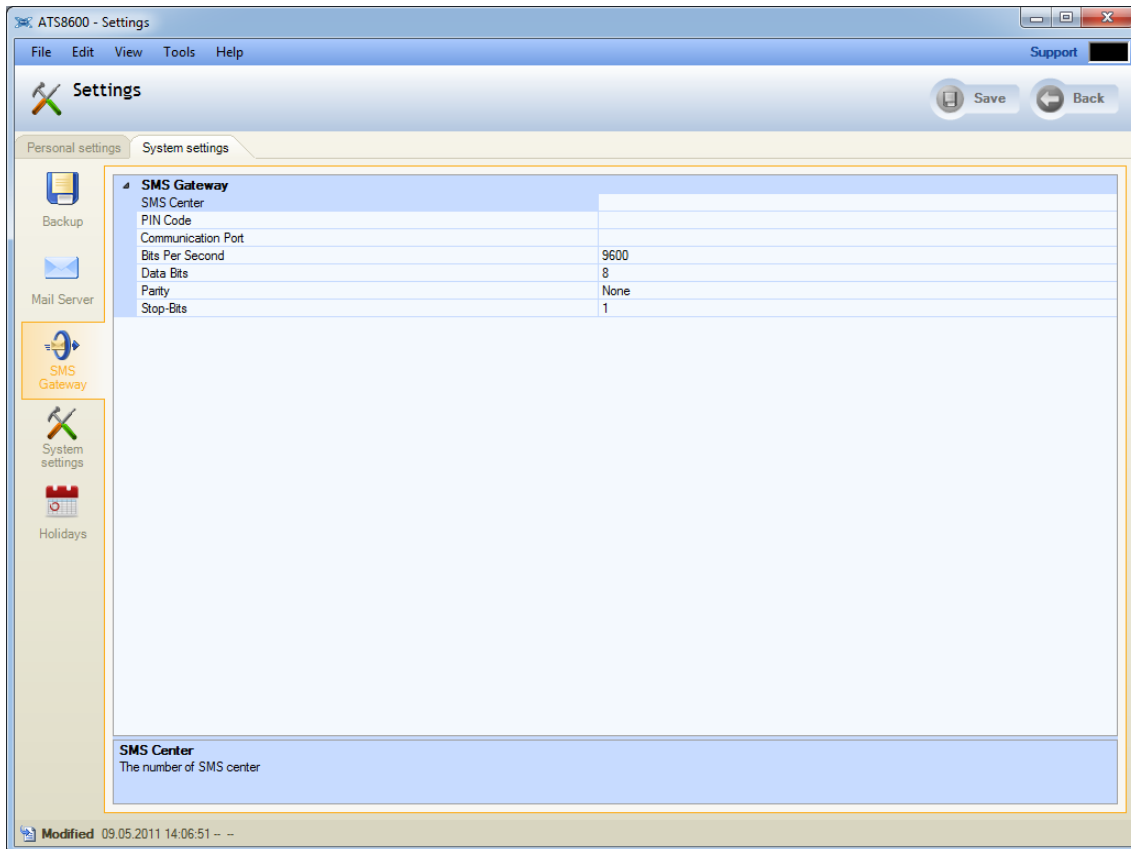


Figure 16-32 SMS gateway parameters

16.2.2.1 Changing the SMS gateway Settings

SMS central unit

If the SMS central unit does not contain a predefined telephone number, enter the number given to you by the operator. Otherwise, this field is left blank.

PIN

If the SIM card is locked by a PIN code, you need to enter the PIN code into settings, so that the driver would be able to unlock it.

Tip:

We recommend not to have a SIM PIN code to prevent the system being locked because all attempts to enter a correct PIN failed and the SIM card is locked.

Communication port

This indicates a server serial port that is used to communicate with the SMS gateway:

(Bits per second, Data, bits, Parity, Stop bits)

Detailed setup of the serial port is set according to a specific SMS gateway.

Communication port must be set as COM + number. (e.g., COM1, COM2.....COMn)

Note:

If the communication port and its parameters are set up incorrectly, SMS functionality will not

activate.

Warning:

After changing the settings, the services must be restarted in a specified order:

1. Stop *Device Manager* and then *Message Broker*.
2. Start *Message Broker* and then *Device Manager*.

17 Visits

The *Visits* module is used to administer cards handed out to customers. It is used to register visitors as well as the host and allows tracking the card handed out.

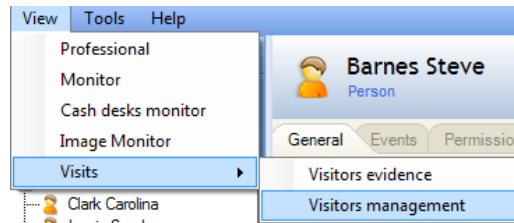


Figure 17-1 Selecting a menu option

17.1 Visitors management

This part controls the entire *Visits* module.

Procedure for initialising the *Visits* module:

1. Creating a reception.
2. Define the accesses concerning the visiting cards sets belonging to this reception;
3. Assign the visiting cards sets;
4. Issue the command for sending persons to devices.

17.1.1 Create a reception

A reception is a group of workplaces sharing the same visiting cards sets. Receptions are created in order to centralise the visitor management of a specific company within ATS8600. Different receptions cannot see visits of other receptions.

It is necessary to create at least one reception, as it is not possible to produce visitor evidence without reception.

To create a reception:

1. Click the *Root* node in the *Visitors management* tab in the *Receptions* tree. Right-click and select the *Add - Reception* function.

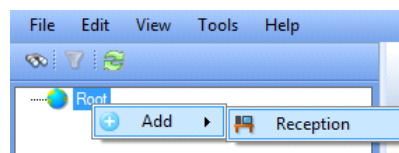


Figure 17-2 Creating a reception

2. Enter the reception details and confirm.

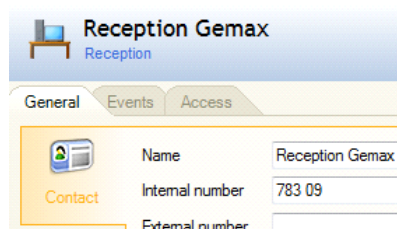


Figure 17-3 Entering reception details

If there are two or more receptions present in the system, when entering the *Visitors* module, a user will be asked to choose the reception that he/she wishes to use and register visitors into.

17.1.2 Define accesses for reception's visitor cards

To set the access for visitor card sets managed by the respective reception, click on the *Access* tab on the right-hand side of the selected *Receptions* tree. You can set the access the same way as in persons access rights settings described [in chapter Personal Settings](#).

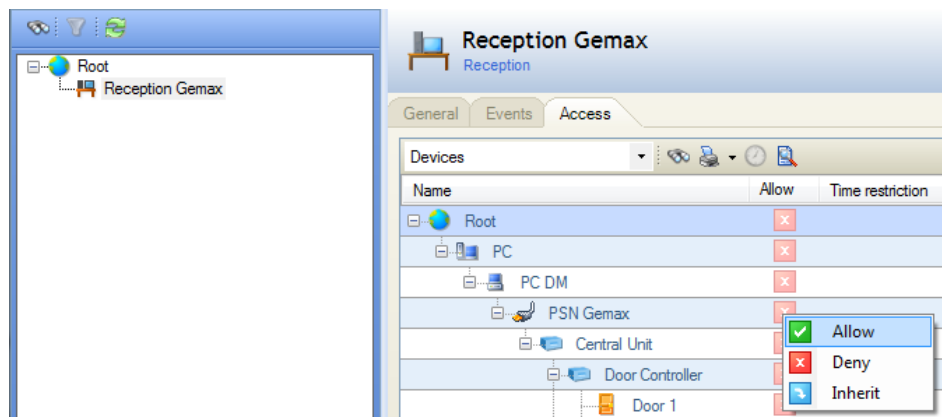


Figure 17-4 Setting access to reception's cards

In this manner you can define the devices through which the visitor obtaining the card is allowed to pass.

Tip:

It is not recommended to allow visitors to access private company premises. Restricted access only - i.e., access to public premises (passage, dayroom, etc.) - is recommended.

17.1.3 Assign visitor cards to a reception

Assigning visitor cards to a reception is performed in the card management infotype.

1. Click the **Add** button to select the card you wish to assign to the reception.

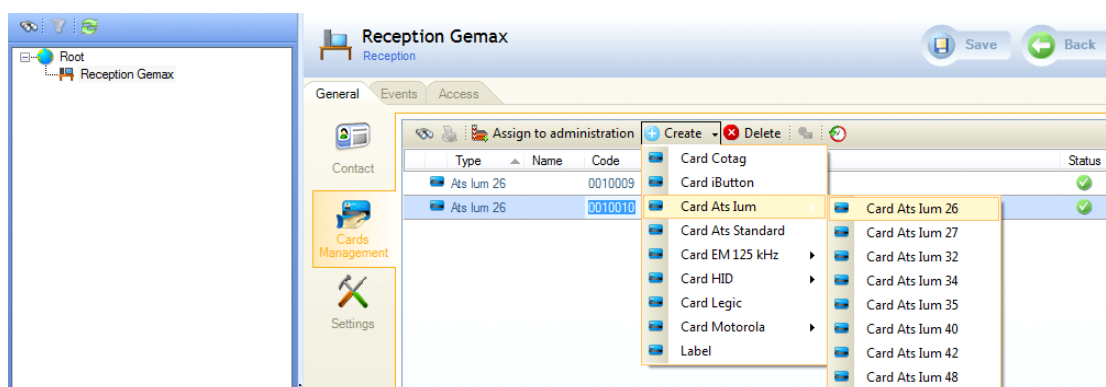


Figure 17-5 Assigning a visitor card to the reception

2. Enter the information about the card: *Name* and *Code* and **Save**.

Type	Name	Code	Holder	Status
Ats Ium 26		0010009		✓
Ats Ium 26		0010010		✓
Ats Ium 26		0010011		✓

Figure 17-6 Assigned cards

In this list you can manage the visitor cards

- *Search*
- *Assign to administration*
- *Create*
- *Delete*
- *Sort by column*

Visitor card management follows the rules similar to the management of cards - credentials. These operations are described [in chapter Credentials Management in the OS environment](#). However, do not use visitor cards as normal employee cards and vice-versa.

17.1.4 Issuing a command for card loading

Cards need to be activated before being handed out to visitors. Cards are send to devices automatically daily at a set time or may be send manually to devices by selecting the **Send credentials** operation in the *Devices* tree; [see chapter Credential activation](#).

17.1.5 Importing visitor cards

Visitor cards can be imported into the system in a similar way to employee cards. The procedure is described [in chapter Credentials import](#).

17.1.6 Reception settings

Individual settings for each reception in ATS8600 can be performed in the *Visitors management* panel on the *Settings* tab. For example, you can set up whether *Host* details are mandatory in the visits register of the given reception. Various receptions in the system can therefore have different settings.

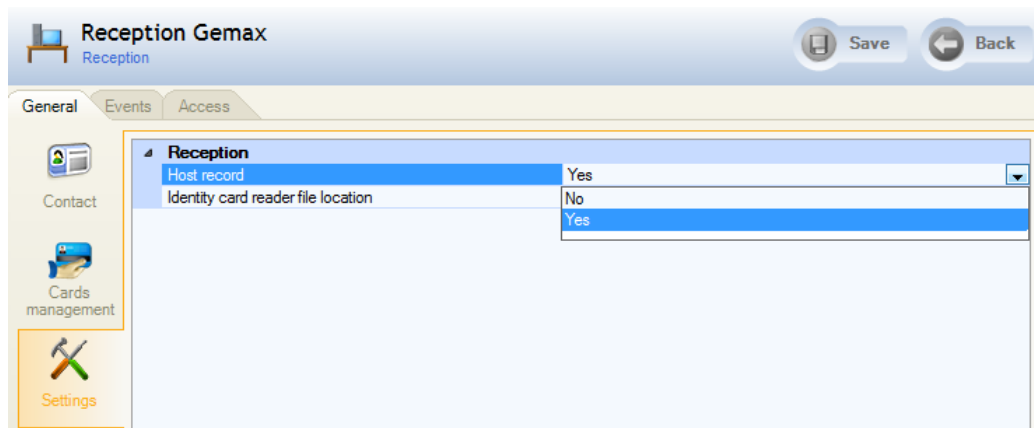


Figure 17-7 Reception settings

In the reception, the path to the file with visitor data collected from a reader can also be set.

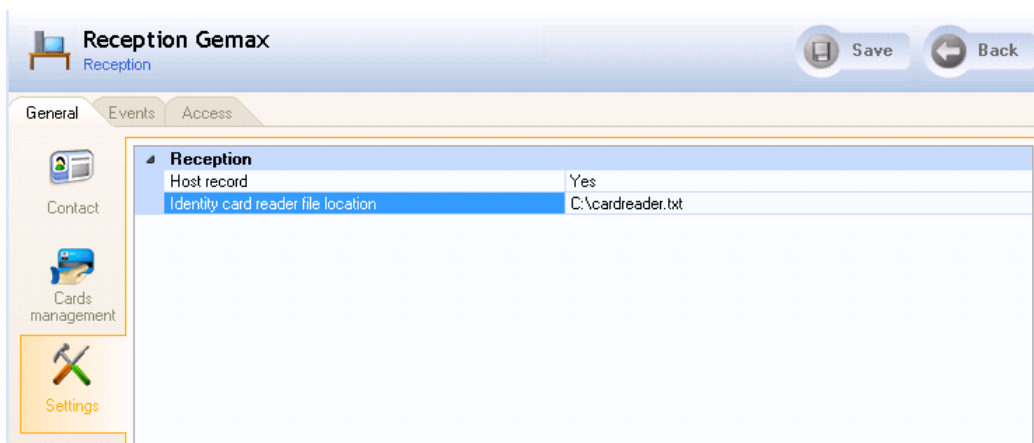


Figure 17-8 Setting a file path from a reader

17.1.7 Defining various access rights within one reception

If it is necessary to define different access permissions for certain visitor cards, it can be done by using corridors.

A corridor is an element that can be created under a reception and has the same configurable properties as the reception.

Under the reception, create a new corridor that represents a delimited area to which the specified group should have access (e.g., second floor).

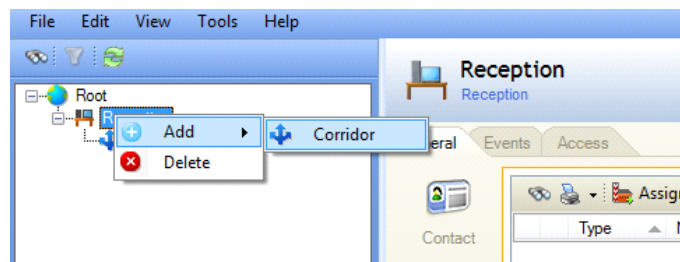


Figure 17-9 Creating a corridor under the reception

Add visitor cards that will have access to the specified areas to the corridor management.

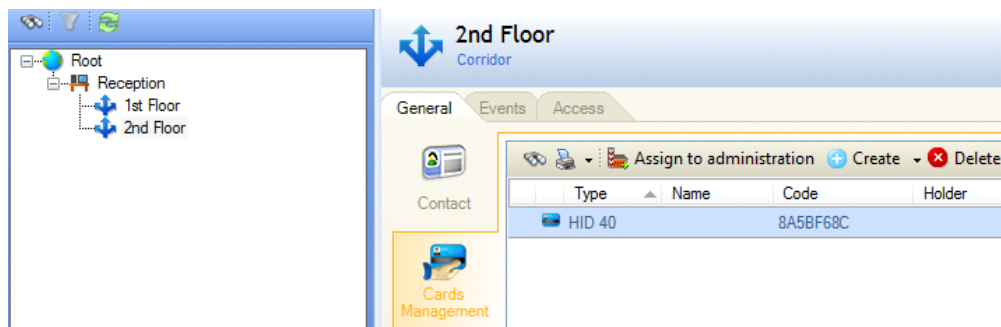


Figure 17-10 Assigning visitor cards to the corridor

Define the access permission on the corridor.

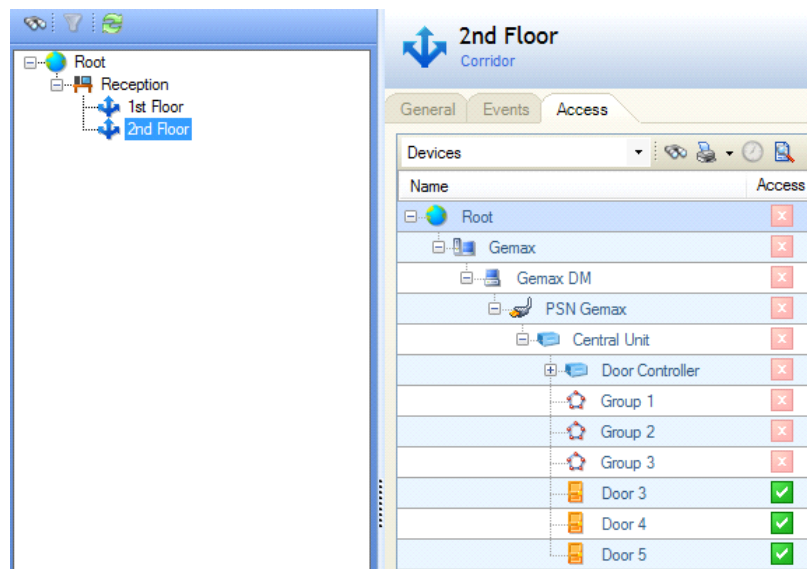


Figure 17-11 Allowing access to the corridor

After persons are send to their respective central units, access permissions of visitor cards are valid and can be assigned to visitors on the *Visitors evidence* record panel.

17.2 Visitors evidence

Visitors are recorded through visitor evidence.

When registering a new visit, proceed as follows: in the main menu select *View - Visits - Visitors evidence*. The window with the list of current visitors displays. The list can be sorted by any column by clicking its name.



Figure 17-12 List of current visits

17.2.1 Quick adding a new visit

A new visit can quickly be registered by badging the card in front of the card reader. The system will then create a new visitor record. The window with pre-populated data will be shown. The reception then clicks  to fill in the visitor card and clicks **Enter** twice to confirm the entered data.

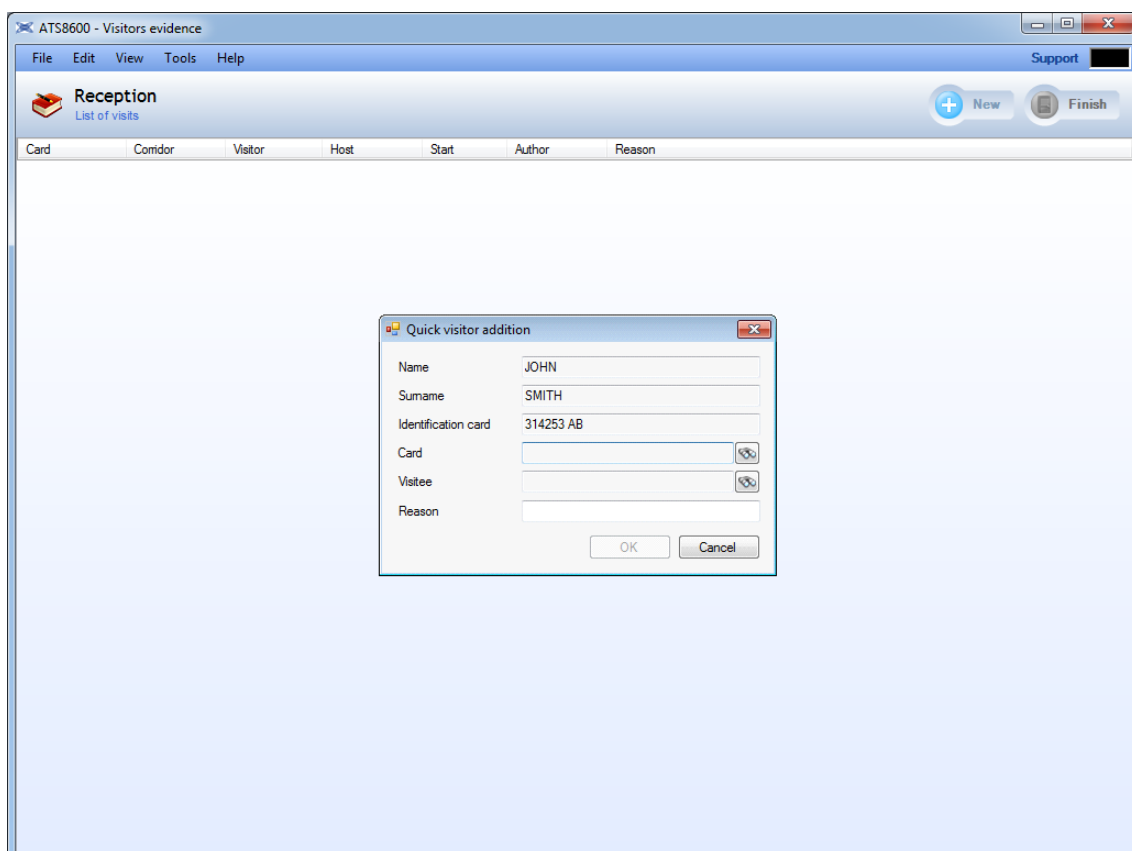


Figure 17-13 Quickly registering a new visit

Warning:

For ID card readers, fill in the path to the file containing data from this reader ([see chapter Reception settings](#)).

17.2.2 New visitor record

A new visitor can be registered after the reception has taken down a new record for a visit:

1. By clicking  in the visits list.
2. The window for visit lookup entering will open. Enter the name, a part of the name or the ID card number and click .

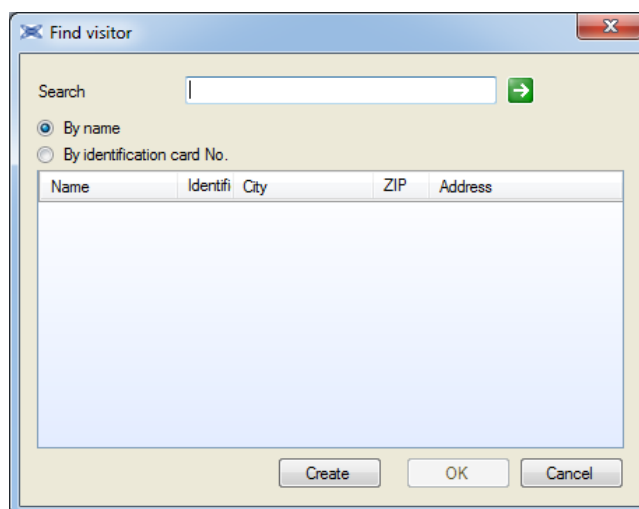


Figure 17-14 Visit search window

3. If the system finds the person (visitor), it means that that person is already registered in the reception and it is not necessary to register that person again. Confirm the visit record.
4. If the system does not find the person, it means that that person has not been registered in the reception yet and he/she must be registered. Continue by clicking **Create**.
5. Enter at least the required information about the visit. Some details showing the  icon can be entered by selecting existing records from a list. This means that clicking this icon displays a list of options you can choose from. In the case the required recording is not included in this list, enter the details manually into the respective field.

Example:

The name of a visitor visiting the company for the first time needs to be registered into the system in order for the system to "remember" that person's name. When the person next visits, the visitor can be looked up according to his/her name (by clicking the  icon and double-clicking their name) and the name will be inserted into the respective field. Searching of existing visitors is not accent-sensitive.

Warning:

You can fill in the *Host* field only by selecting an existing employee from the list. New employees cannot be added.

The *Host* property can be mandatory or optional. It depends on the configuration of the reception.

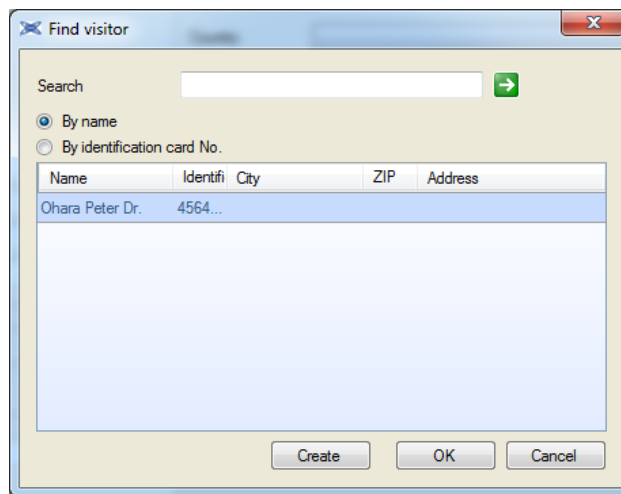


Figure 17-15 Selecting from the list of existing records

Figure 17-16 Form for registering visits

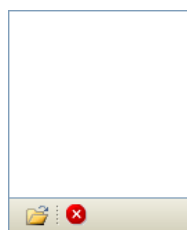


Figure 17-17 Picture import

The visitor's picture can be assigned to his/her account - [see chapter Adding a picture to a person's record](#).

If the reception registers a person who the system administrator has declared to be an not allowed person, the system will warn the user not to issue the card to that person. It is up to the receptionist to decide whether the visitor in question will be allowed to enter the premises despite the warning.

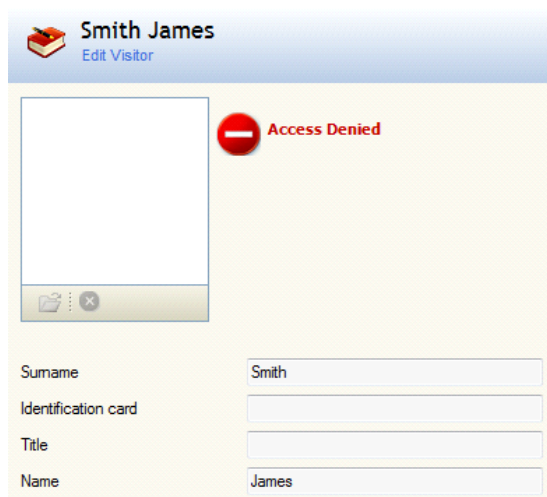
The screenshot shows a web interface for editing a visitor's record. At the top, there's a header with a small icon and the text 'Smith James' and 'Edit Visitor'. Below this is a large empty box for a picture, with a red circle and a minus sign next to it, and the text 'Access Denied' in red. To the right of the picture box are four input fields: 'Surname' with 'Smith' entered, 'Identification card' (empty), 'Title' (empty), and 'Name' with 'James' entered.

Figure 17-18 Visitor with denied access to the object

The visitor's contact information is displayed on the right-hand side of the screen. You can register additional information in the *Extended* tab.

The screenshot shows the 'Extended' tab of the visitor form. It has two tabs: 'Contact' and 'Extended'. The 'Extended' tab is active. It contains several input fields: 'Company', 'Car number', 'Car type', 'Parking place', 'Expiration reason', and 'Note'.

Figure 17-19 Extended tab - additional information about the visitor

After registering all mandatory and relevant data about the visit, click the  button to save the record. The visit is registered into the current list of visits.

17.2.3 Finishing the visit

At the end of the visit, it is necessary to inform the ATS8600 system and formally close the visit.

Select the required record in the list of visits and click the  button in the upper right corner. The record will disappear from the list of visits. The card can now be issued to another visitor;

information about the visitor is recorded in the system's history.

Note:

Several receptionists can work together in one *Visits* module; i.e., they all can enter visits into the system. The screen is updated every five seconds.

17.2.4 Modifying visitor's data

Visitor data can be further modified in the *Visitors* tree of the *Visitors management* module. To allow a person to modify the tree, assign permissions in *Application -> Visits -> Visitors management*.

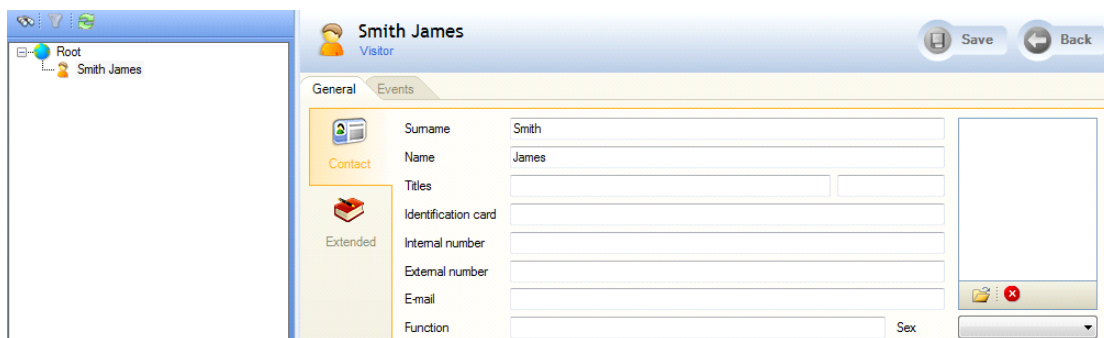
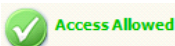
The screenshot shows a web application interface for managing visitors. On the left is a tree view with 'Root' and 'Smith James'. The main area is titled 'Smith James Visitor' and has 'Save' and 'Back' buttons. It features two tabs: 'General' (selected) and 'Events'. Under the 'General' tab, there are two sections: 'Contact' and 'Extended'. The 'Contact' section includes fields for Surname (Smith), Name (James), Titles, Identification card, Internal number, External number, E-mail, and Function. The 'Extended' section is currently empty. A 'Sex' dropdown menu is located at the bottom right of the form.

Figure 17-20 Visitors tab in Visitors management

The  icon indicates the permitted access of the visitor. Click this button to configure for a particular person that the receptionist does not allow this person to enter the object in the future. As a result of this setting, the specified visitor will be marked with the  icon.

Warning:

The  button is only informative; this setting does not prevent the person from entering the object.

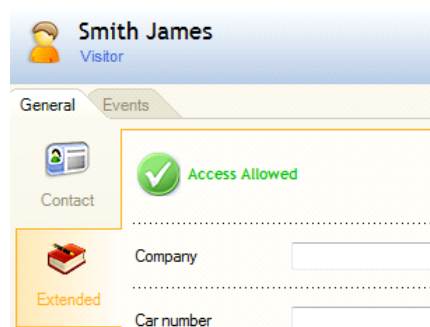
This screenshot shows the 'Advanced' properties of a visitor named 'Smith James'. The 'General' tab is selected, and a green checkmark icon with the text 'Access Allowed' is prominently displayed. Below this, there are two sections: 'Contact' and 'Extended'. The 'Extended' section contains fields for 'Company' and 'Car number', both of which are currently empty.

Figure 17-21 Advanced properties of a visitor with allowed access to the object

Tip:

Receptions can use visiting tickets as well as credentials. Visiting tickets are simple credentials without electronic chips and they are most commonly filled out by hand. Although these visiting tickets are not sent to access devices, they make it possible to search for entry and exit of visitors in reception's events.

Tip:

Visits events history can be viewed and printed in *Visitors management* panel. Else the window will hide automatically if another window becomes active.

18 Data import and export

Data import and export enables users to transfer data between two ATS8600 System implementations or between two different information systems.

When importing and exporting data the ATS8600 System uses data saved in XML format. Data can also be imported from Excel ([see chapter Person import from Microsoft Excel](#)).

Data export makes it possible to extract information and data saved in the system and consequently save it in a form that enables further use of the data. All information about persons, credentials, and devices can be extracted into groups and roles, along with all information about devices of the ATS8600 system user interface. Importing allows a user to insert information entered in the required format from a file into the ATS8600.

The import and export function offers a variety of possibilities:

- In terms of the integration of a company's personnel system into the ATS8600, you can import persons' data into the *Persons* tree of the ATS8600.
- Import and export of persons is extended by the option to import and export permissions.
- This function allows an existing list of devices to be imported into the *Devices* tree of the ATS8600, which is especially useful when performing large-scale installations with many devices.
- It also allows to import and export the *Regions* tree configurations and to preserve the created region configuration.
- It allows you to export and import the existing configuration for instance from a test environment into the (live) production environment.

Import and export of these configurations must be performed in the following order:

1. *Persons*
2. *Devices*
3. *Regions*
4. *Credentials*
5. *Permissions* (Permissions are always imported after the persons, devices, regions, and identifiers have been deployed within the application.)

18.1 Data export

Data can be exported from the ATS8600 In a complex way, i.e., the data of an entire tree, or partially, i.e., only the data of a selected node, or of a selected object.

1. If you want to export the configuration of the *Persons* tree together with all information, click to select the *Root* node. Select *External data - Export* from the *File* menu.

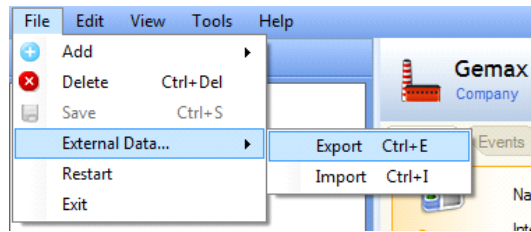


Figure 18-1 Import and export

2. Select *Person export to file* in the displayed window and click **Next**.

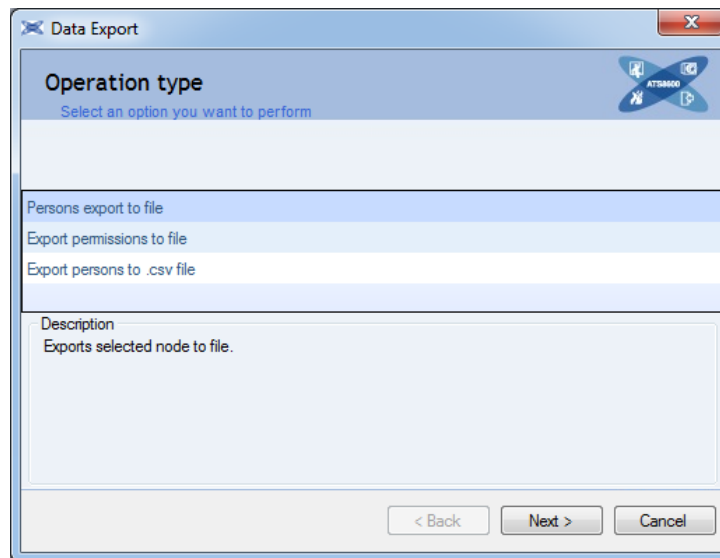


Figure 18-2 Export to file

3. In the next window open the location to which you wish to export the data file. To export data on groups and subordinates, check the respective boxes.

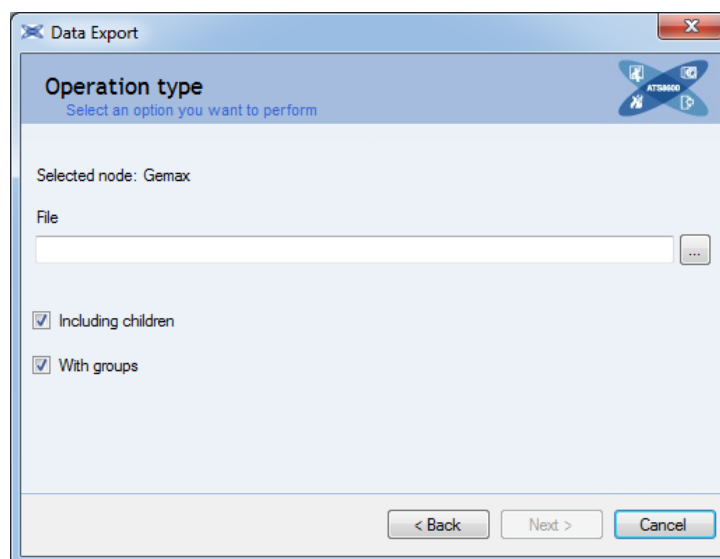


Figure 18-3 Selecting location for data export

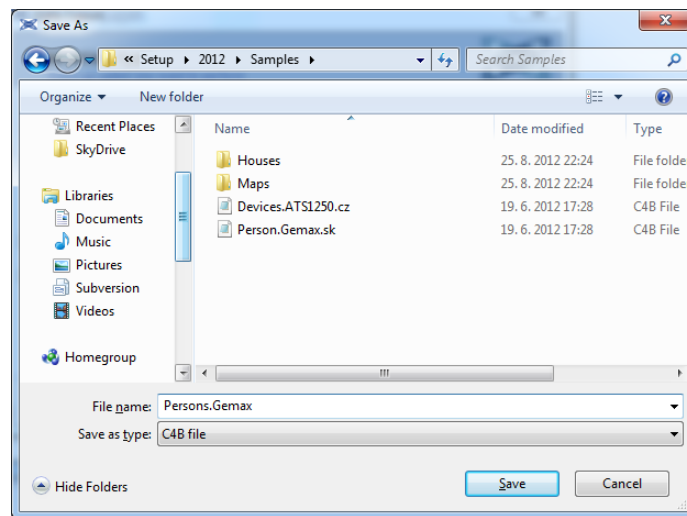


Figure 18-4 PC folder structure

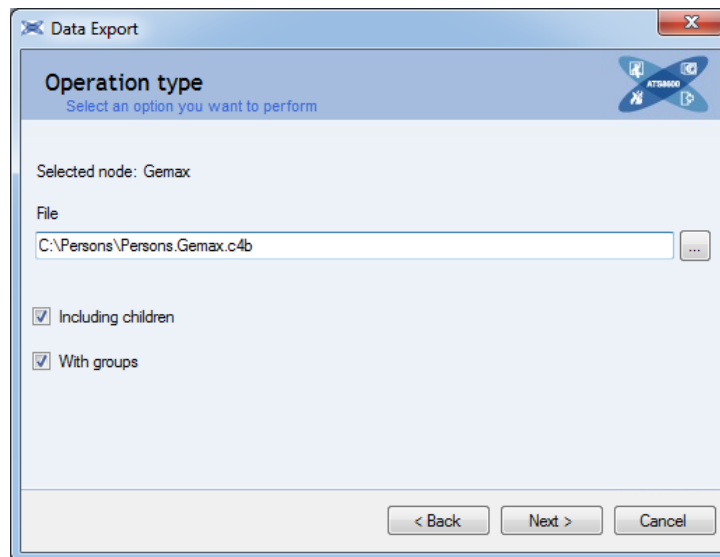


Figure 18-5 Export settings

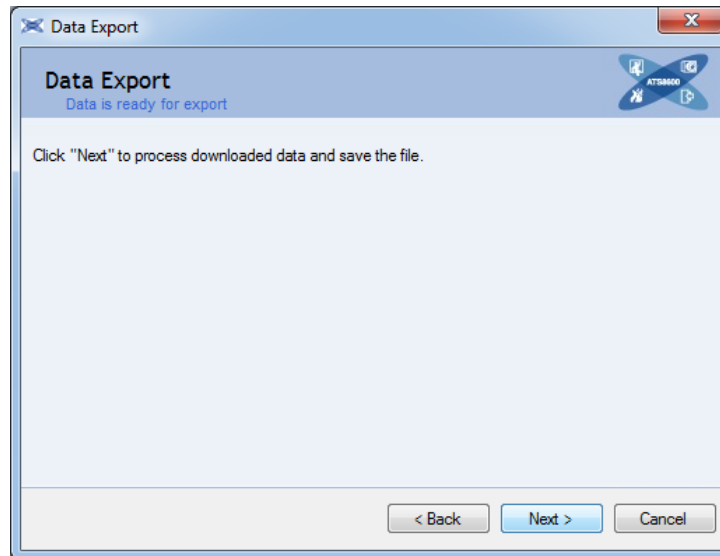


Figure 18-6 Selection to execute the export

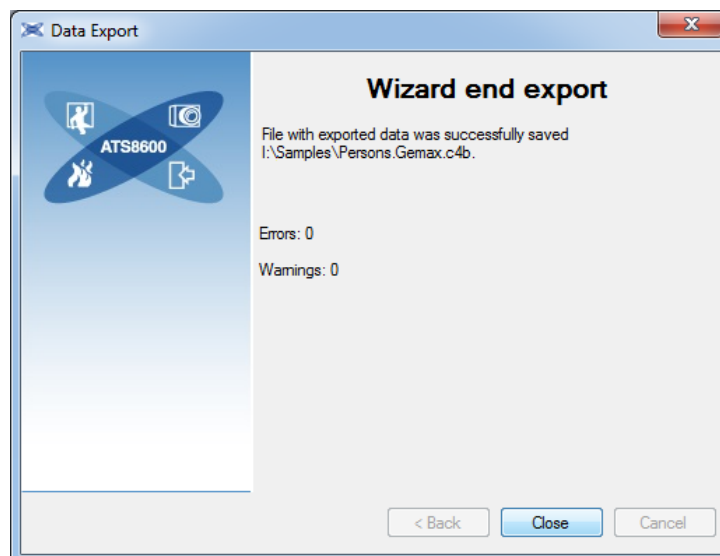


Figure 18-7 Finishing the export wizard

Follow a similar procedure when exporting devices or regions. However, when exporting devices, choose the *Devices* tree. You can export regions only in the *Regions* tree.

Note:

Exporting PINs

When exporting PINs, the user must have permission in *Application* to display PINs. It is not advised to enable this for security reasons.

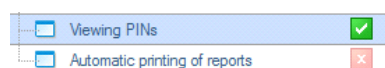


Figure 18-8 User permission setting for viewing PINs

18.2 Importing Data from a File

1. To import the configuration of the *Persons* tree together with all information, click to select the *Root* node. Then select *External data - Import*.

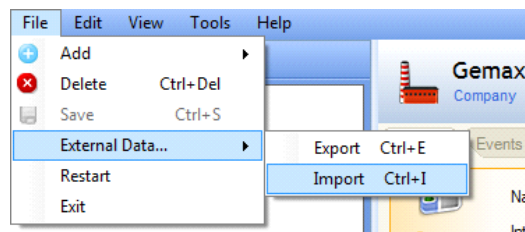


Figure 18-9 Import and export

2. In the displayed window, select *Person import from file* or *Credentials import from file*.

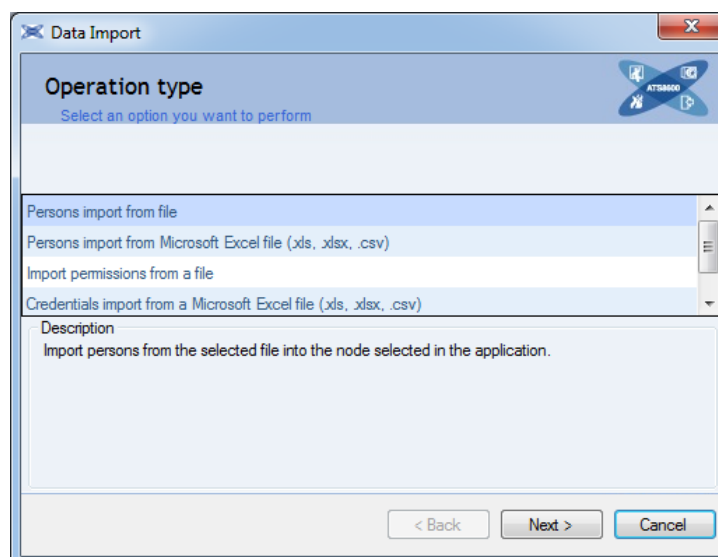


Figure 18-10 Import from a file

3. Select a file located on the hard disk. Next, select whether you want to resolve collisions caused by importing persons from a file into an application.

Persons who collide because they are not the same in both the file and the application will be identified in the system by matching identifiers.

As an identifier, you can use one of the following two options:

- **Person ID**
A number automatically assigned by the application. This is a good option if no other means for person identification exist within the organisation.
- **Internal number**
If you mark persons within an organization by unique codes like personnel number or HR number, these can be entered in the Internal number field in the *Contact* tab. At import, you can select to identify based on the Internal number field.

If a match between credentials of a person from the file and a person from the application is found,

select one of the following three options:

- Create new
Persons from the file with the same ID as a person from the application will be imported, but they will receive new IDs.
- Replace existing
Persons from the file that have the same ID as a person from the application will be imported, but the original persons in the application will be deleted (overwritten).
- Synchronization
Persons in the application that have the same IDs as the persons from the file will be overwritten as well, like in the previous case. Moreover, persons who are in the application, but not on file will be deleted.

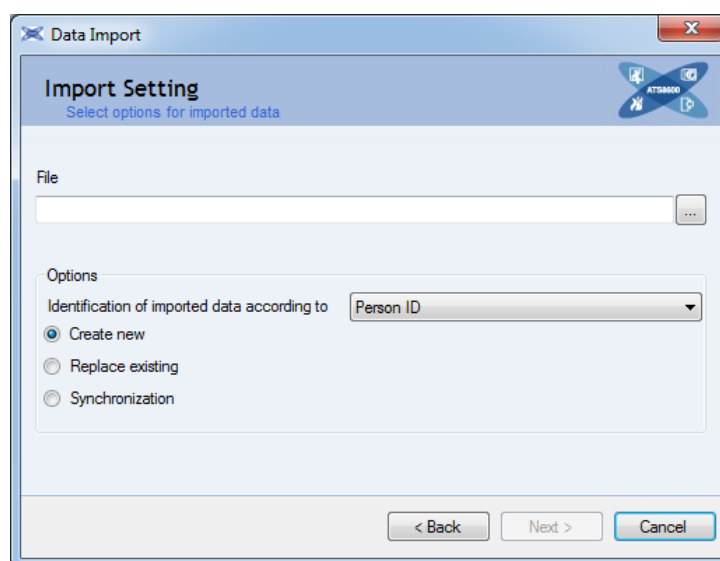


Figure 18-11 Setting import options

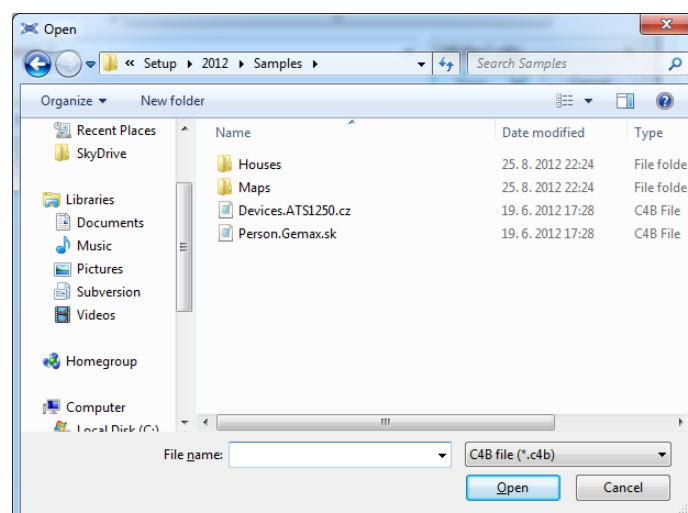


Figure 18-12 Selecting and inserting an imported file

Further steps are similar to the export procedure ([see chapter Data export](#)). Confirm and finish the operation. The application window will subsequently be generated anew and new data will be imported

into the *Persons* tree.

Proceed in a similar manner when importing devices or regions. However, when importing devices, select the *Devices* tree. When importing regions, select the *Regions* tree.

18.2.1 Person import from Microsoft Excel

A list of persons can be imported from an Excel table into ATS8600 application. ATS8600 supports .xls format of Excel XP and 2003.

The Excel table format with the list of persons you wish to import into the ATS8600 application must meet the following requirements:

- Column names in the first row of the table are data that will be imported to the ATS8600 application (e.g., first name, surname, personal number, centre name, card type, etc.). These names are arbitrary.
- Only two columns are mandatory: *Surname* and *Internal number* (personal number);
- *Internal number* must be unique for each person, duplicates are not allowed. If personal numbers are identical, the ATS8600 system will create only the last one.
- *Internal number* may be repeated only if importing more cards for one person.
- Columns must be of the same data type (number, text, etc.). Changing the data type is described at the end of the chapter - see warning.

If the table contains more persons with the same surname but a different personal number, two persons with the same surname will be created.

	A	B	C
1	Department	Internal Number	Surname
2	TestDepartment		1 TestPerson1
3	TestDepartment		2 TestPerson2
4			3 TestPerson3
5			4 TestPerson4

Figure 18-13 Example of an Excel table

If a "Centre" node type has been created in the *Persons* tree and persons in the table are assigned to a centre, the persons list from the table will be imported directly under this centre. If the centre is not created, the persons will be created under the company.

How to import:

1. The .xls file the data will be imported from cannot be opened during the import.
2. In the *Persons* tree, create a company to which the person list will be imported.
3. Select Import.
4. Select the option to import from a file and confirm.
5. In the Import settings window browse your PC for the file you wish to import.

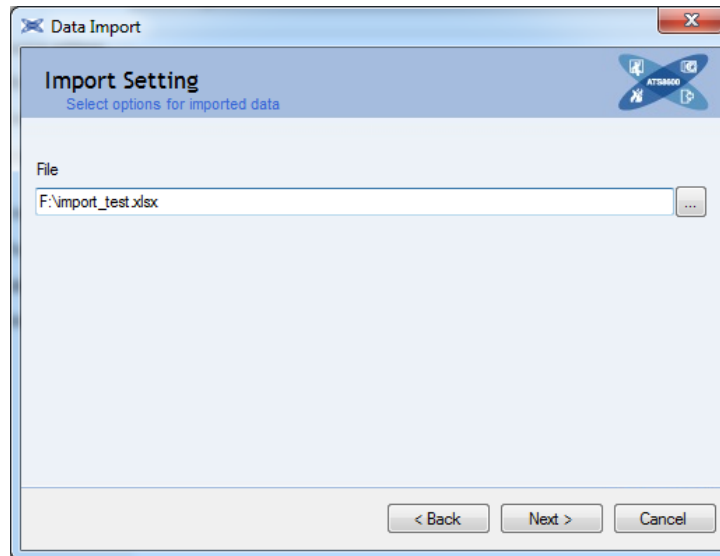


Figure 18-14 Setting persons import

6. Select a file located on the hard disk. Choose from further options whether you wish to replace existing data with the imported data, create a new configuration or synchronise data.
7. The next window shows data from an Excel file. You need to assign Excel items to items in ATS8600. It is required to assign *Internal number* and *Surname* fields. No other data needs to be assigned.

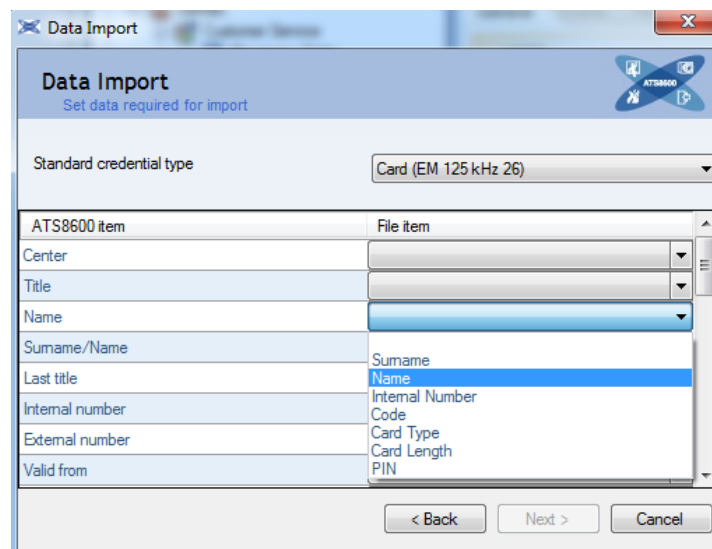


Figure 18-15 Assigning attributes

Warning:

Generally, *Internal number* is recorded in Excel as a number. In cases when the personal number contains a letter or a special sign, Excel saves the data as a different attribute type.

	A	B
1	Surname	Internal Number
2	TestPerson1	100 25
3	TestPerson2	100 26
4	TestPerson3	N - 100 27

Figure 18-16 Example of a different data type

If importing persons from Excel into the ATS8600 system, all data must be of the same attribute type. Here is how the data can easily set to be of the same attribute type in Excel:

1. Mark all cells in the opened Excel sheet with the data prepared for import to ATS8600.
2. Right-click and select **Format cells**.

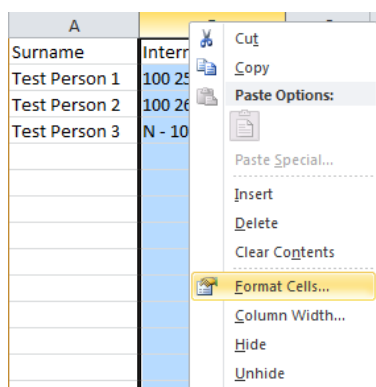


Figure 18-17 Data type setting function

From the menu select the *General* data type and confirm.

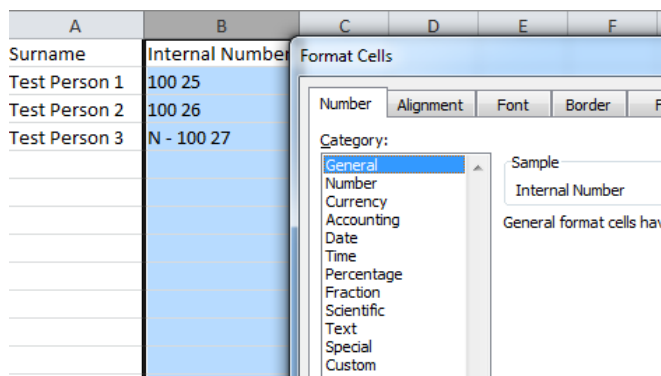


Figure 18-18 Selecting the data type

Such data can be imported into the ATS8600 system correctly.

If the Excel table contains two or more identical names and personal numbers but different card numbers, the system creates one person with several assigned cards.

In this way, more cards may be assigned to one person at the same time. Cards can be imported also individually, [see chapter Credentials import](#).

List of items in ATS8600:

Center (for centre import)
Internal number (required)
Title
Firstname
Surname (required)
2. title
E-mail
Identification card
BIN
VAT
Web
Note
Invoice address
Function
Sex
ZIP code
City
Fax
Cellphone
Phone
Work phone
Address

For credentials:

Card name
Card code (required for card import)
Card type
Card length

18.2.1.1 Credentials import

Importing cards into the system is performed using the Credentials import from a Microsoft Excel file (.xls) function.

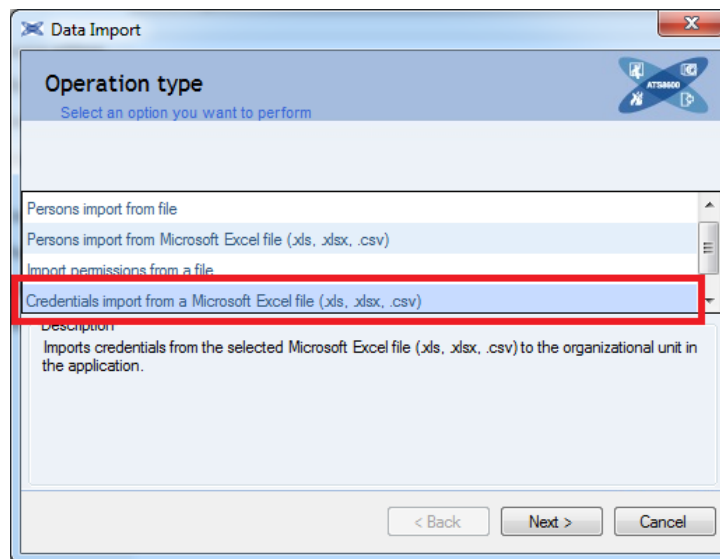


Figure 18-19 Importing cards from Excel

To import cards, the type and length of the cards must be specifically defined (e.g., ATS IUM 32). Visitor cards can also be imported.

The procedure for importing people with cards is exactly the same as described [in chapter Person import from Microsoft Excel](#).

Note:

If you experience problems with card importing or the import fails, check the following:

1. Check that the *Code* column is filled for the rows containing the data of the identifiers you want to import.
2. If an incorrect card type is created, check whether the correct card type and length has been entered according to the list of supported credentials in the ATS8600 Integrated Security Management System.
3. If the last page shows: *"You cannot import credential with the same data!"* - this means that you are trying to import an existing credential.

Warning:

The application does not currently support importing between different ATS8600 Integrated Security Management System versions.

19 Licensing

A license enables the client (user) to use the ATS8600. The ATS8600 is not limited by license according to the number of users but according to the number of connected devices.

In general, only the persons logged into the system as administrators or support and persons with the Administrator role can perform the licensing operations.

Select *License* from the *Help* menu. The *Licensing* window opens.

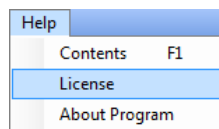


Figure 19-1 License activation Licensing

The window with information on the current license appears:

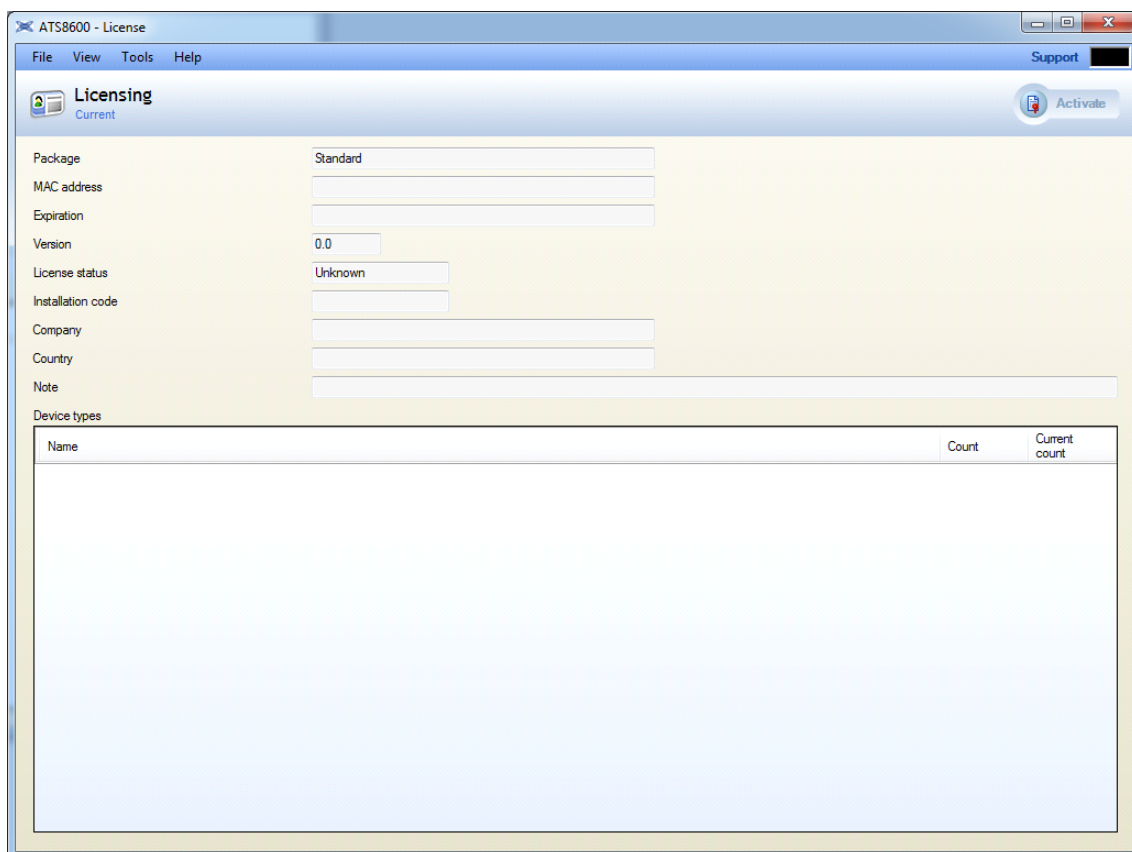
A screenshot of a software window titled 'ATS8600 - License'. The window has a menu bar with 'File', 'View', 'Tools', and 'Help'. On the right side of the menu bar is a 'Support' button. Below the menu bar is a 'Licensing' section with a 'Current' status and an 'Activate' button. The main area of the window contains a form with the following fields: 'Package' (set to 'Standard'), 'MAC address', 'Expiration', 'Version' (set to '0.0'), 'License status' (set to 'Unknown'), 'Installation code', 'Company', 'Country', 'Note', and 'Device types'. The 'Device types' section contains a table with three columns: 'Name', 'Count', and 'Current count'. The table is currently empty.

Figure 19-2 Licensing

1. If you own a demo version of the ATS8600 and you do not have a license, the details in this window will be empty.
2. If you already own a license, the attributes in the *Licensing* window contain the current license information. To connect further devices to this system, you need to update the license. The license will be received in the form of an activation key from the supplier of your ATS8600 Integrated Security Management System, upon fulfilling the licensing conditions.

Warning:

The device list contains only the devices included in the activated licence and those with their drivers installed. In case of a licence activated for a device that is not included on the list, install the respective device driver.

The License panel contains the following information:

- *Edition* - software product edition that defines available functions.
- *Network card address* - device hardware identifier with an activation key assigned to it.
- *Expiration* - the expiration time for a license limited by a certain period of time.
- *Version* - software product version for which the license is issued.
- *License status* - the status of the given license.
- *Installation code* - distinct installation identifier
- *Company* - license owner.
- *State* - state in which the owner of the license resides.

Device types: the window contains a list of all licensed devices. Each entry contains the following information:

- *Count* - maximum number of devices allowed of that type. If you need to increase the number of allowed devices, contact your provider.
- *Current count* - number of running devices of the given type.

Note:

See the product web page to view ATS8600 licensing.

19.1 License activation

You will receive the license to the ATS8600 system from your supplier in the form of an file with extension .lic. To activate it, click **Activate** in the upper-right corner of the screen in the *Licensing* tab.

The window to browse your PC for the license file will appear.

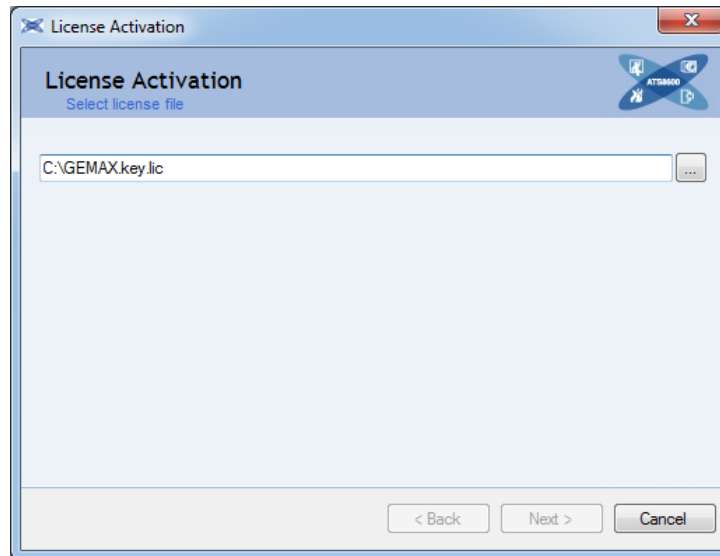


Figure 19-3 Selecting the license file

If the verification of the license file is successful, activate the key by clicking **Next** to activate the key.

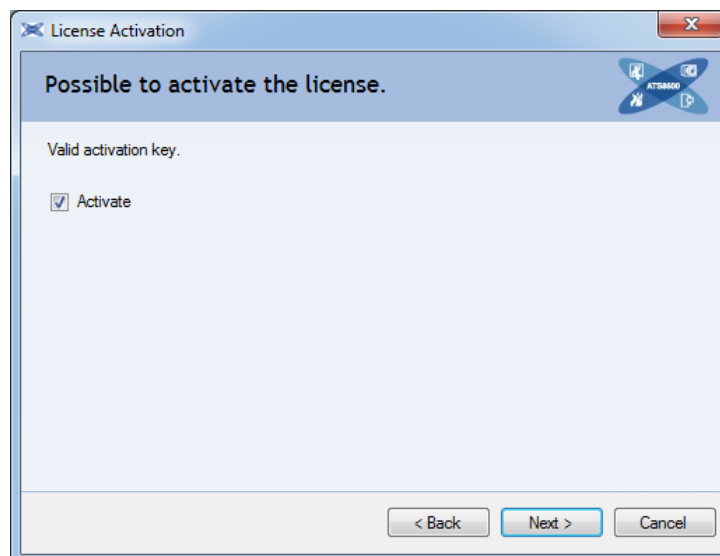


Figure 19-4 License activation

Finish the license activation. The activated license will automatically enter the respective information into the *Licensing* window: data on the activation key, names and numbers of devices.

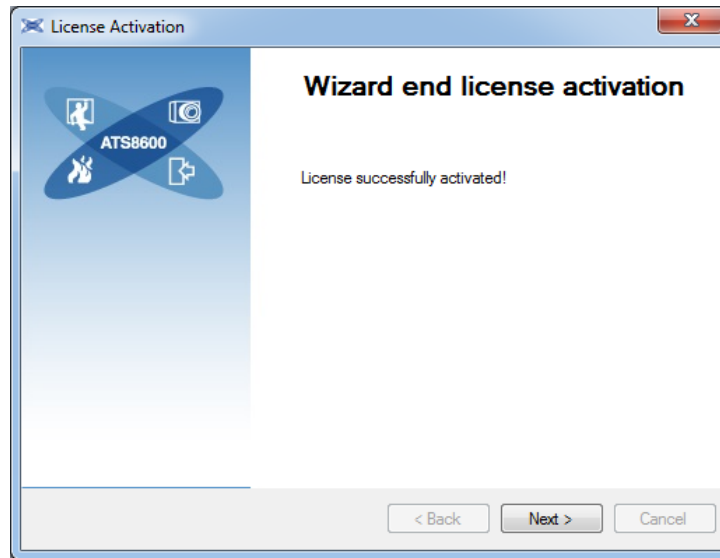


Figure 19-5 Finishing the license activation

20 Diagnostics view

This view is used to manage diagnostic files and for the overview of ATS8600 server components that run in the background. Diagnostics may be helpful for technical support to diagnose issues that would take too long using regular methods. *Diagnostics* is located in the *Tools* menu.

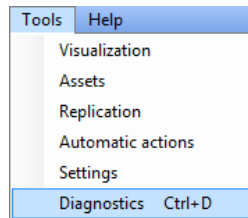


Figure 20-1 Diagnostics view

20.1 System components overview

The ATS8600 Server consists of three components: *Device Manager*, *Message Broker*, and *Replication Manager*. These components are programs that run in the background (also called system services). Their status can be monitored in the first section of this panel. Each component can be in one of three states:

- Running - service is running 
- Stopped - service is stopped 
- Blocked - service is blocked 

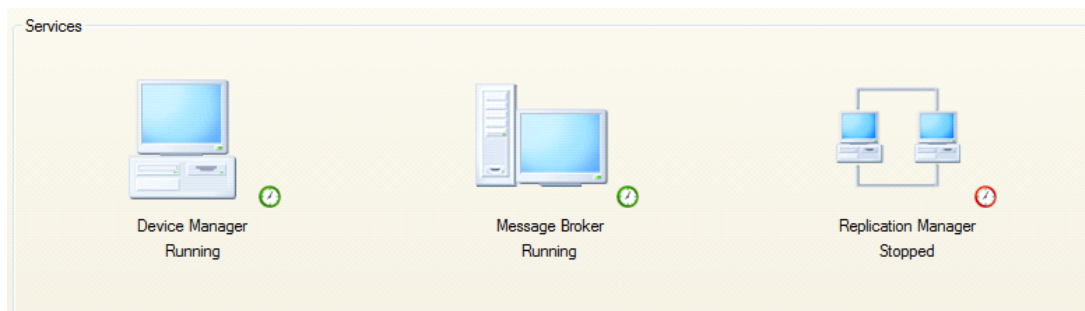


Figure 20-2 Services overview

The **Refresh** button is used for updating the panel. If the panel has been opened for some time, we recommend using it to obtain updated information about the services' states, logging method, size, and the location of the log directory.

20.2 Log management

The *Diagnostics* panel provides multiple options for log management.

1. Press Turn on Trace to enable the diagnostic mode used mostly to diagnose device communication problems. To turn off this mode press Turn off Trace.

2. The system provides the information about the log size, which indicates the log file volume on the disc.

Example: Log size: 118.3 KB

3. You can set a folder for storing all log files. Enter the folder path into the text field and press Set directory ☒.

4. To delete the log folder, press Delete log files.

5. To download the log folder contents, press Download log files. After pressing the button, you need to select the name of the .zip archive and the location on the hard disk where the contents would be downloaded. The log folder files are compressed into this archive.

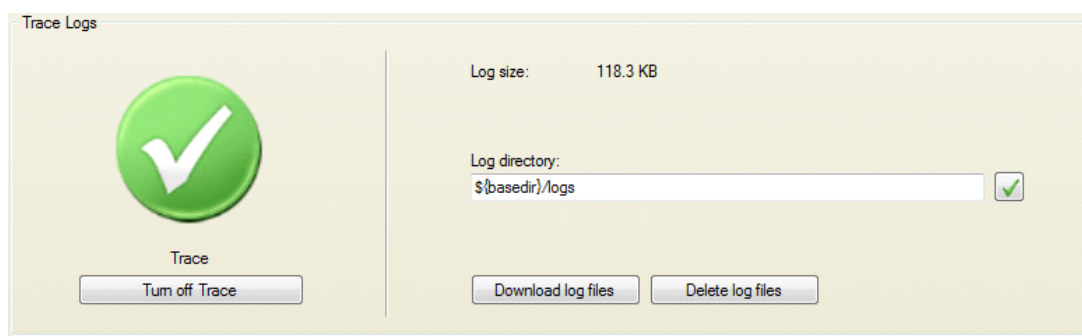


Figure 20-3 Trace logging

21 Data Backup in ATS8600

One of the main features of the main database is easy data maintenance. ATS8600 uses the standard MS SQL 2008 database. This enables you to integrate ATS8600 into internal company processes of data back-up.

The production database contains current configurations and event history for the time period defined for the particular project. The time period of the history saved influences the hardware requirements of the server (memory and hard disks). This database is backed up regularly in order to be available in case of a server failure. If backups are enabled, ATS8600 backs up all data each day at 11 p.m. If you need to set up back-up intervals or back-up methods, contact your database administrator.

To backup the production database, set the backup. In *Tools*, select the *Settings* module. After the module starts, select *System settings*. In Back-up, enter the following back-up attributes:

1. *Enabled* - select Yes to run the automatic back-up according to preset parameters.
2. *Directory* - folder on the database server where database backups will be stored.

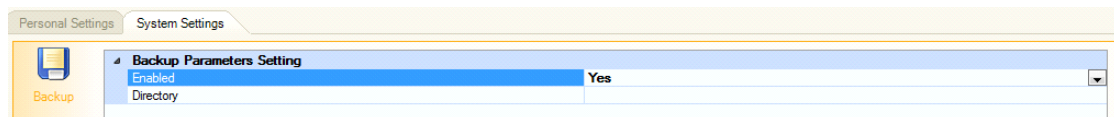


Figure 21-1 Setting of back-up parameters

After saving the settings, automatic ATS8600 database backups are activated. Files with database backups are stored on the server in the defined folder. The complete backup files always contain the last three backups. These files are overwritten automatically and continuously.

Note:

We recommend using this method to back up the database, only if the installation runs the free MS SQL Express edition that does not include automated database jobs. If the standard database server edition, which makes it possible to create automatized database jobs, is available for the installation, we recommend using its jobs to set the backup. This edition offers more detailed back-up settings that can help optimize the database workload in case of large back-up files. To create the database jobs, consult the database server administrator.